DECLARATION OF PAUL SCHWARTZ ISO GOOGLE, LLC'S OPPOSITION TO PLAINTIFF'S MOTION FOR CLASS CERTIFICATION AND APPOINTMENT OF CLASS REPRESENTATIVES AND CLASS COUNSEL

Unredacted Version of Document Sought to be Sealed

QUINN EMANUEL URQUHART & SULLIVAN, LLP
Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Sara Jenkins (CA Bar No. 230097)
sarajenkins@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Andrew H. Schapiro (admitted *pro hac vice*)
andrewschapiro@quinnemanuel.com
Teuta Fani (admitted *pro hac vice*)
teutafani@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
Crystal Nix-Hines (Bar No. 326971)
crystalnixhines@quinnemanuel.com
Alyssa G. Olson (CA Bar No. 305705)
alyolson@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

Josef Ansorge (admitted *pro hac vice*)
josefansorge@quinnemanuel.com
Xi ("Tracy") Gao (CA Bar No. 326266)
tracygao@quinnemanuel.com
Carl Spilly (admitted *pro hac vice)*
carlspilly@quinnemanuel.com
1300 I Street NW, Suite 900
Washington D.C., 20005
Telephone: (202) 538-8000
Facsimile: (202) 538-8100

Jomaire Crawford (admitted *pro hac vice*)
jomairecrawford@quinnemanuel.com
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Jonathan Tse (CA Bar No. 305468)
jonathantse@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Attorneys for Defendant Google LLC

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA, OAKLAND DIVISION

CHASOM BROWN, WILLIAM BYATT, JEREMY DAVIS, CHRISTOPHER CASTILLO, and MONIQUE TRUJILLO, individually and on behalf of all similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 4:20-cv-03664-YGR-SVK

DECLARATION OF PAUL SCHWARTZ IN SUPPORT OF GOOGLE, LLC'S OPPOSITION TO PLAINTIFF'S MOTION FOR CLASS CERTIFICATION AND APPOINTMENT OF CLASS REPRESENTATIVES AND CLASS COUNSEL

Judge: Hon. Yvonne Gonzalez Rogers
Hearing Date: September 20, 2022
Hearing Time: 2:00 p.m..

I, Paul Schwartz, declare as follows:

1. Counsel for Defendant Google, LLC retained me to provide expert analysis and, if requested, expert testimony in this matter.

2. I submit this declaration in support of Google's Opposition to Plaintiff's Motion for Class Certification.

3. Attached as Exhibit 1 is a true and correct copy of the Expert Report of Professor Paul Schwartz, dated June 7, 2022. The opinions I provided therein are true and correct to the best of my knowledge.

I declare under penalty of perjury of the laws of the United States that the foregoing is true and correct. Executed in Berkeley, CA on Aug. 1, 2022

By Paul Schwartz
Paul Schwartz

EXHIBIT 1

Redacted Version of Document Sought to be Sealed

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA – OAKLAND DIVISION

CHASOM BROWN, WILLIAM BYATT, JEREMY DAVIS, CHRISTOPHER CASTILLO, and MONIQUE TRUJILLO, individually and on behalf of all similarly situated, Plaintiffs, v. GOOGLE LLC, Defendant.	Case No. 4:20-cv-03664-YGR-SVK

EXPERT REPORT OF PROFESSOR PAUL SCHWARTZ

June 7, 2022

TABLE OF CONTENTS

Page

I. Executive Summary Of Opinions.

1. After reviewing Jonathan E. Hochman and Bruce Schneier's expert reports, I have reached the following conclusions based on my expertise in information privacy principles, regulations, FTC guidance, and existing standards:

2. **Opinion # 1: Mr. Hochman's opinions on PI, PII, and identifying information are contrary to U.S. information privacy standards**. Mr. Hochman adopts definitions of PI, PII, and identifying information, which are far-reaching, indeterminate, and contrary to U.S. information privacy standards, including (1) guidance from the Federal Trade Commission (FTC Guidance), (2) the ALI Data Privacy Principles, and (3) the California Consumer Privacy Act (CCPA). Furthermore, Mr. Hochman's categorical approach fails to exclude data that is non-identifying, and is therefore over-inclusive. American information privacy standards require a contextual approach to determine whether a (i) "GET request," (ii) IP address, (iii) "fingerprint" data, (iv) "User-ID," (v) geolocation data, and (vi) information in "Google cookies" are non-identifying or likely to identify. However, Mr. Hochman fails to conduct—or propose a reasonable plan to conduct—the contextual analysis required to determine whether the Data at Issue[1] is reasonably linkable to, or "identifying information" for, a particular individual or class member. He also fails to consider Google's policies and guidelines that affect whether the Data at Issue can reasonably be linked to an identified individual.

[1] This term refers to the data plaintiffs claim Google improperly receives from communications between users and websites when users are in "private browsing mode" and not signed into a Google Account and visit a web-site that uses Google services (hereafter, "the Data at Issue"): (i) "GET request" sent from the user's computer to the website; (ii) the IP address of the user's connection to the internet; (iii) information identifying the browser software that the user is using, including any "fingerprint" data; (iv) any "User-ID" issued by the website to the user, if available; (v) geolocation of the user, if available; and (vi) information contained in "Google cookies," which were saved by the user's web browser on the user's device at any prior time.

3. **Opinion # 2: Although Mr. Schneier does not adopt Mr. Hochman's categorical approach to PI, PII, and identifying information, his report suffers from similar defects because he opines that even if identifying information is absent, data could be identified through additional sources**. In particular, Mr. Schneier opines that PI is any information that identifies or theoretically could be linked with an individual or their household, such as name, email, social security number, internet browsing history, etc.[2] He also opines that non-PII can turn into PII "whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available [non-PII] information, could be used to identify an individual."[3] By ignoring Google's practices, as established in publicly available policies and practices, Mr. Schneier's approach is contrary to U.S. information privacy standards.

4. **Opinion # 3: The Data at Issue is not personally identifying, there is a low probability of identification by Google, and the Data at Issue is exempt from data subject access requests**. That Google may in some circumstances have sufficient information to identify some individuals cannot establish *on a class-wide basis* that the Data at Issue is PI, PII, or "identifying information" and there is a low probability that Google could individually identify users. Even if the plaintiffs were able to establish that it was PI or PII under certain circumstances, individualized factual inquiries would still be necessary to determine whether the Data at Issue is PI or PII for any given class member.

---

[2] Schneier ¶ 81.

[3] Schneier ¶ 80.

II. Personal Background And Qualifications.

5. I am the Jefferson E. Peyser Professor of Law at the University of California at Berkeley School of Law in Berkeley, California. I am also a Director of the Berkeley Center for Law and Technology (BCLT).

6. I received my law degree from Yale Law School, where I served as a senior editor of the Yale Law Journal. My undergraduate studies were at Brown University. I also carried out post-graduate legal studies in data protection law at the Johann Wolfgang Goethe University in Frankfurt-am-Main, Germany, as a fellow of the Alexander von Humboldt Foundation.

7. My scholarship examines the legal, regulatory, and policy implications of a wide variety of areas of information privacy and security. These include consumer privacy, data security breaches, spyware, cloud data, comparative privacy law, the international diffusion of privacy law, tax privacy, the conflict between privacy law and trade law, and other topics. At Berkeley Law School, I teach courses in information privacy, cybersecurity law, and tort law. I have been teaching information privacy law for thirty-four years, and I taught one of the very first courses in this area in the United States.

8. I have written several books, including the leading casebook INFORMATION PRIVACY LAW (7th ed., 2020), which is used at over twenty law schools, as well as the distilled guide PRIVACY LAW FUNDAMENTALS (6th ed., 2022). Daniel Solove, Professor of Law at George Washington University Law School, is my co-author on both of these books. My most important scholarly publications regarding information privacy include: *Privacy and/or Trade*, 90 UNIVERSITY CHICAGO L. REV. – (forthcoming 2023) (co-author Anupam Chander); *ALI Data Privacy: Overview and Black Letter Text*, 68 U.C.L.A. L. Rev. 1252 (2021) (co-author Daniel Solove); *Global Data Privacy: the EU Way*, 94 N.Y.U. LAW REVIEW 771 (2019); *Legal Access to*

Global Cloud Data, 118 COLUMBIA LAW REVIEW 1681 (2018); *Transatlantic Data Privacy Law*, 106 GEORGETOWN LAW JOURNAL 115 (2017) (co-author Karl-Nikolaus Peifer); *Reconciling Personal Information in the U.S. and EU*, 102 CALIFORNIA LAW REVIEW 877 (2014) (co-author Daniel Solove); *The EU-U.S. Privacy Collision*, 126 HARVARD LAW REVIEW 1966 (2013); *Information Privacy in the Cloud*, 161 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 1623 (2013); *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. LAW REVIEW 1814 (2011) (co-author Daniel Solove); *Preemption and Privacy*, 118 YALE LAW JOURNAL 902 (2009); and *Property, Privacy, and Personal Data*, 117 HARVARD LAW REVIEW 2056 (2004).

9. My scholarship is often cited as an authority on data privacy. For example:

- My 2004 Harvard Law Review article, *Property, Privacy, and Personal Data*, was cited in plaintiffs' Complaint (see Second Amended Complaint ¶ 125, *Brown v. Google*, 5:20-cv-03664-LHK (2021), Dkt. 136-1; Third Amended Complaint ¶ 125, *Brown v. Google*, 5:20-cv-03664-YGR (2022), Dkt. 395-2). This same article was also cited in plaintiffs' Complaints in *Calhoun v. Google*,[4] and by plaintiffs in *In re: Facebook, Inc. Internet Tracking Litigation*, 2012 WL 12369553 at ¶ 114 (N.D. Cal. May 23, 2012).
- My co-authored 2011 N.Y.U. Law Review article, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, was cited in the 2012 FTC Report, "Protecting Consumer Privacy in an Era of Rapid Change."[5]

[4] *Calhoun v. Google*, 4:20-cv-05146-YGR-SVK Dkt. 1 ¶ 215; Dkt. 163 ¶ 218; Dkt. 302-3 ¶ 213.

[5] Federal Trade Commission (F.T.C.) Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, 20, n.107 (March 26, 2012), https://perma.cc/L2LX-4LEC, *citing* Paul M. Schwartz & Daniel J. Solove, *The PII Problem:*

10. My expert opinions have been solicited in matters in federal and state courts in the United States. Google also engaged me to serve as an expert in the related case, *Calhoun v. Google*. In December 2021, I submitted an expert report in *Calhoun* responding to the information-privacy related opinions of the plaintiffs' expert, Dr. Zubair Shafiq, who was writing in support of plaintiffs' motion for class certification.[6] I also provided deposition testimony as an expert in the *Calhoun* matter.

11. In a past engagement, the Commissioner of Insurance of the State of California engaged me as a privacy expert to assist in litigation defending a California law, the Holocaust Victim Insurance Relief Act of 1999 (HVIRA). My expert activity on this matter included assisting the State of California with an affidavit supporting the HVIRA and explaining why, in my judgment, German data protection law did not prohibit the insurance companies in that matter from sharing insurance information pursuant to this statute. The United States Supreme Court ultimately invalidated HVIRA as a violation of the federal foreign affairs power.[7]

12. I have testified before the U.S. Congress, the California State Assembly, and served as an advisor to the Commission of the European Union and other international organizations. In 1990, I became the first American to address the annual meeting of the world's data protection commissioners, the International Conference of Data Protection and Privacy Commissioners (now

---

Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814, 1836–1848 (2011).

[6] Because Mr. Hochman's and Mr. Schneier's reports recapitulate many of Dr. Shafiq's arguments regarding personal information and personally identifiable information, I have drawn on my previous report in Calhoun v. Google to rebut their arguments. *See* 5:20-cv-05146-LHK, Dkt. 430-1, Exhibit 3 (hereinafter, "*Calhoun* Rebuttal Report").

[7] *See American Ins. Ass'n v. Garamendi*, 539 U.S. 396 (2003).

called the Global Privacy Assembly). My presentation on the state of American privacy law was delivered at their conference held in the French Senate in Paris.

13. I have testified before the California Assembly in an Informational Hearing concerning "Balancing Privacy and Opportunity in the Internet Age," held on December 12, 2013 at the University of Santa Clara. My writings and classes have examined many questions involving California privacy law. *See, e.g.*, DANIEL SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 102-106; 821-832; 970-973 (7th ed. 2020); Paul Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 816-817 (2019); *Foreword*, in LOTHAR DETERMANN, CALIFORNIA PRIVACY LAW xxv (4th ed. 2020).

14. For several years, I have focused my teaching and scholarship on the California Consumer Privacy Act ("CCPA"). In addition to teaching the CCPA's provisions in my information privacy class, cybersecurity class, and privacy seminar, I have also discussed it in recent articles, such as *ALI Data Privacy: Overview and Black Letter Text*[8] *and Global Data Privacy: The EU Way*.[9]

15. I am often quoted by media outlets on issues relating to privacy and technology. Publications in which I have been quoted include *The New York Times, the Washington Post, the Wall Street Journal, the Los Angeles Times, Forbes*, and *Law360*.

[8] Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA Law Review 1252 (2022), at http://dx.doi.org/10.2139/ssrn.3457563.

[9] 94 N.Y.U. Law Review 771 at 816–817 (2019).

16. At the American Law Institute (ALI), I served as a co-reporter on the Data Privacy Principles Project.[10] As the ALI explains, the project seeks "to provide a framework for regulating data privacy and for duties and responsibilities—best practices—for entities that process personal data."[11] Founded in 1923, the ALI is "the leading independent organization in the United States producing scholarly work to clarify, modernize, and otherwise improve the law."[12] Over the course of its history, the ALI has been responsible for such major path-breaking projects as the Restatement of Torts, the Uniform Commercial Code, the Model Penal Code, and the Principles of Corporate Governance.

III. My Assignment.

17. I have been retained by Defendant Google, LLC in the above-captioned matter to evaluate certain sections of the reports of plaintiffs' experts, Jonathan E. Hochman and Bruce Schneier. The first opinion of my report addresses Mr. Hochman's conclusions regarding ***personal information*** ("PI"), ***personally identifiable information*** ("PII"), ***identifying information, entropy, and fingerprinting***,[13] which are relevant to Opinions 2, 9, 10, 14, and 22 of his report. The second opinion of my report addresses Mr. Schneier's conclusions regarding PI, PII, identifying information, and fingerprinting. The second opinion relates to Opinions 3, 7, 8, and 9

[10] *See* The American Law Institute, "Principles of the Law: Data Privacy" (https://perma.cc/986V-87QA); *see also* Solove, Daniel J. and Schwartz, Paul M., *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA Law Review 1252 (2022).

[11] The American Law Institute, "Principles of the Law: Data Privacy" (https://perma.cc/986V-87QA).

[12] *About ALI*, The American Law Institute (2022), https://www.ali.org/about-ali/.

[13] "[F]ingerprinting is the use of unique or probabilistically unique combinations of one or more device, network, or app/browser attributes to identify a device, app, browser, or user across distinct transactions where no persistent unique identifier is explicitly provided by a user's device, app, or browser." GOOG-CALH-00027147 (Privacy Policy – Device/App/Browser Fingerprinting and Immutable Identifiers Policy).

of Mr. Schneier's report. The third opinion rebuts the analysis Mr. Hochman and Mr. Schneier applied and analyzes the Data at Issue under the correct U.S. information privacy standards. The third opinion concludes that the Data at Issue in this litigation is not personally identifying; there is a low probability of Google identifying users from the Data at Issue; and the Data at Issue is exempt from certain data breach notice requirements as well as data subject access rights. The third opinion explains that to rebut the conclusion that the Data at Issue is not PII, individualized determinations would be required to establish the probability that Mr. Hochman's proposed "fingerprinting" would allow for particular users to be identified.

18. I understand that expert Georgios Zervas will discuss Mr. Hochman's opinions relating to descriptions of Google's web services and client-side data practices (Opinions 1, 2, 3, 4, 5, 6, 10, 15, 26, 27, 28, and 29) and expert Konstantinos Psounis will rebut Mr. Hochman and Mr. Schneier's opinions regarding Google's server-side data practices (Mr. Hochman Opinions 4, 5, 6, 9, 10, 14, 18, 19, 20, 22, 23, 24, 26, and 31; Mr. Schneier Opinions 3, 6, 9).

19. With respect to the class action litigation, I understand that plaintiffs Chasom Brown, William Byatt, Jeremy Davis, Christopher Castillo, and Monique Trujillo allege that Google violated various statutes and privacy laws. Specifically, plaintiffs allege that Google "unlawfully intercepted users' private browsing communications to collect personal and sensitive information … without disclosure or consent."[14] Plaintiffs claim that "Google intercepts and collects this data by causing the user's web browsing software to run Google software scripts … that replicate and send the data to Google servers … even if the user is not engaged with any Google site or functionality and even when the user is in a private browsing mode … [without]

[14] TAC ¶ 4.

notice to the user of Google's data collection methods."[15] Plaintiffs further allege that Google's receipt of certain categories of information gives rise to liability, including unauthorized disclosure, breach of contract, invasion of privacy, theft, and unauthorized access of personal information. A purported violation of the CCPA is not one of plaintiffs' causes of action. The CCPA is referenced throughout the Complaint and by plaintiffs' experts, however, and I will therefore discuss it as one of several standards for determining whether data should be considered to be "personal information."

20. Plaintiffs claim that "Google has gained a complete cradle-to-grave profile of users" by "tracking, collecting and intercepting users' (including plaintiffs' and class members') personal communications indiscriminately[.]"[16] Plaintiffs claim that Google improperly receives the following types of data from communications between users and websites when users are in "private browsing mode" and not signed into a Google Account and visit a web-site that uses Google services (as indicated above, "the Data at Issue"): (i) a "GET request" sent from the user's computer to the website; (ii) the IP address of the user's connection to the internet; (iii) information identifying the browser software that the user is using, including any "fingerprint" data; (iv) any "User-ID" issued by the website to the user, if available; (v) geolocation of the user, if available; and (vi) information contained in "Google cookies," which were saved by the user's web browser on the user's device at any prior time.[17]

21. Plaintiffs further allege that the "[i]nformation collected from Google Cookies … includes identifying information regarding the user from private browsing sessions and non-private

---

[15] TAC ¶ 5.

[16] TAC ¶ 93.

[17] TAC ¶ 63 (emphasis added).

browsing sessions, across multiple sessions."[18] Plaintiffs also allege that Google collects "***[i]dentifying information*** regarding the consumer from various Google fingerprinting technologies that uniquely identify the device, such as X-Client-Data Header, GStatic, and Approved Pixels."[19]

22. I understand that plaintiffs are proposing two classes for this lawsuit:

> **Class 1** – All Chrome browser users with a Google account who accessed a non-Google website containing Google tracking or advertising code using such a browser and who were (a) in "Incognito mode" on that browser and (b) were not logged into their Google account on that browser, but whose communications, including ***identifying information*** and online browsing history, Google nevertheless intercepted, received, or collected from June 1, 2016 through the present (the "Class Period").
>
> **Class 2** – All non-Chrome browser users with a Google account who accessed a non-Google website containing Google tracking or advertising code using any such browser and who were (a) in "private browsing mode" on that browser, and (b) were not logged into their Google account on that browser, but whose communications, including ***identifying information*** and online browsing history, Google nevertheless intercepted, received, or collected from June 1, 2016 through the present (the "Class Period").[20]

23. I am being compensated for my work at the rate of $1,215 per hour. My opinions in this matter are in no way dependent on my compensation or the outcome of this case.

---

[18] *Id.* ¶ 93 (emphasis added).

[19] *Id.* ¶ 93 (emphasis added).

[20] TAC ¶ 192.

IV. Opinion # 1: Mr. Hochman's Opinions Are Contrary To Information Privacy Standards.

A. Mr. Hochman Fails To Distinguish Between Non-Identifying Data And Data That Is Reasonably Likely To Identify.

24. Mr. Hochman's report adopts categorical definitions of PI and PII.[21] First, with respect to PI, Mr. Hochman claims that "URLs, IP addresses, user agent, referer, and other information from the user's private browsing communications" are "personal information" that Google collected throughout the class period.[22] In a separate passage, he states that "URLs visited," "[i]dentifiers on non-Google websites matched to Brown's Biscotti ID," "[d]evice type," "[o]perating system and version," "[b]rowser type and version," and "[l]anguage" are also personal information that Google collected while a named Plaintiff was logged-out of their account and in private browsing mode.[23]

25. Second, with respect to PII, Mr. Hochman states that in his opinion "an IP address, especially when combined with a user-agent string, constitutes personally identifiable information ("PII") because this data can be used to uniquely identify a user ***with a high probability of success***."[24] Then he provides a definition of PII from a blog post by Corinne Bernstein, Adjunct Assistant Professor in the Department of Humanities at Farmingdale State College: "'Personally

---

[21] *See e.g.*, Hochman ¶ 106 ("[T]he intercepted and collected information in private browsing mode are sensitive, personal information…that…includes data such as IP address, cookie/device ID, PII, postal address, geo-location data etc."); ¶ 174 ("This Google file…contains a myriad of personal information and private browsing activities, including…URLs visited[,] Identifiers on non-Google websites matched to Brown's Biscotti ID[,] Device type[,] Operating system and version[,] Browser type and version[,] Language[,] Location information including latitude and longitude[,] Travel history including number of countries, cities and airports visited[.]").

[22] *Id.* ¶ 99 (emphasis added).

[23] *Id.* ¶ 174.

[24] *Id.* ¶ 105 (emphasis added).

identifiable information (PII) is ***any data that could potentially identify a specific individual***. Any information that can be used to distinguish one person from another and can be used to deanonymize previously anonymous data is considered PII.'"[25]

26. Mr. Hochman assumes a broad and amorphous definition of PII as "any data that could potentially identify a specific individual." In his opinion, Mr. Hochman focuses on a measure known as "entropy," which—according to Mr. Hochman—calculates the "number of bits of data needed to uniquely identify a person."[26] In Mr. Hochman's opinion, the number of required bits globally is 33 "[w]ith a little less than 8 billion people on earth" and "[w]ith around 330 million people in the United States, 29 bits of data is more than sufficient to identify a person."[27] For Mr. Hochman, information—or multiple pieces of information put together—that reach or exceed 29 bits are sufficient to identify an individual in the United States.[28] Under Mr. Hochman's entropy approach, the Data at Issue is therefore PII if it reaches or exceeds a specific threshold (*i.e.*, 29) that can be mathematically calculated.[29]

---

[25] *Id*. ¶ 105 (emphasis added), citing https://perma.cc/37V9-FZGA (last accessed on May 11, 2022) ("[PII] may include the following: name, address, email, telephone number, date of birth, passport number, fingerprint, driver's license number, credit or debit card number, Social Security number").

[26] *Id*. ¶ 231.

[27] *Id*.

[28] *See id*.

[29] In support of *Calhoun* plaintiffs' motion for class certification, Dr. Zubair Shafiq submitted an expert report in which he opines that the Data "uniformly" sent from Chrome to Google at issue in the case is "PI" and "PII." In a similar approach to Mr. Hochman, Dr. Shafiq defines PII by calculating the so-called "entropy" (in bits) of the "minimum amount of information required to uniquely identify" an individual internet user on earth. According to Dr. Shafiq, that number of required bits is 32 and therefore information ("or multiple pieces of information put together") that reaches or exceeds a "32-bit threshold" is PII. *See Calhoun v. Google,* 5:20-cv-05146-LHK, Dkt. 340-19, Report of Dr. Zubair Shafiq; *see also Calhoun* Rebuttal Report.

27. Finally, Mr. Hochman's report treats "identifying information" as information that does not directly identify an individual person, but rather information that *could* be joined with other information to identify an individual. For example, Mr. Hochman acknowledges that the Data at Issue is stored in a way that is not directly linked to a person's Google Account. However, he opines that the Data at Issue could be linked to class members with various "identifying information" such as IPv6 addresses.[30] Elsewhere he states that cookies—one of the types of Data at Issue—"are pieces of 'text stored by a user's web browser' containing ***identifying information*** and used by Google for tracking and advertising purposes."[31] In my opinion, Mr. Hochman's treatment of "identifying information" is contrary to how that term is commonly defined in U.S. information privacy standards.[32] Mr. Hochman's opinion in this litigation on "identifying information" is also contrary to a recent publication by Mr. Hochman, in which he states the following:

> An identifier by itself is meaningless and is just a code. For example, any random combination of nine numbers very well may be a social security number, but without identifying information, there is no relevance, utility or vulnerability. Identifying information alone is not overly relevant, because it simply notes the existence of a person, without any detail of that person.[33]

---

[30] *Id*. ¶ 229 ("Within Google's various logs and storage, IP address, particularly IPv6, can be used to link data from different logs storing signed-out data collected from private browsing and non-private browsing modes to a particular user's device and to the user's signed-in identity and data."); *see* also *id*. ¶ 156 ("As for the private browsing information at issue in this case – where class members are not signed into any Google account – Google stores the data in a way that people have no ability to review or delete that information – with various ***identifying information*** that could be linked to class members and their devices.") (emphasis added).

[31] *Id*. ¶ 108 (emphasis added).

[32] *See, e.g.*, App. C (42 C.F.R. § 426.400, 5 C.F.R. § 581.203, 34 U.S.C.A. § 12291, 22 U.S.C.A. § 2507a, 42 U.S.C.A. § 11360).

[33] Michael J. Fischer, Jonathon E. Hochman, and Daniel Boffa, "Privacy-Preserving Data Sharing for Medical Research," Stabilization, Safety, and Security of Distributed Systems: 23rd

28. **There is no single definition for personal data that applies in all laws and regulations in the United States.** As a matter of comparative privacy standards, this development in the United States is quite different from the situation in the European Union, where there is a single definition of this concept.[34] As illustrated in Appendices A, B, and C, the United States also lacks a single term for the basic idea of personal data: personal information. Terms used to express this concept include: personal identification information, personally identifiable information, nonpublic personal information, personal health information, and electronic personal health information.

29. Increasingly, however, **the U.S. approach to information privacy generally converges around the same touchstone concept: Data falls under information privacy guidelines when it can be "reasonably linked" to an individual.**

30. Mr. Hochman's theory, which is based on a categorical mathematical definition, is contrary to this well-established approach. Although Mr. Hochman's report and supporting materials provide examples of myriad laws, regulations and instruments that use the terms PI and PII, none of these laws, regulations, and instruments even mention the 33-bit (global) or 29-bit (U.S.) formula that Mr. Hochman applies. I am also not aware of any privacy policy, regulation, or court in the United States applying this categorical definition of personal information.

International Symposium, SSS 2021, Virtual Event, https://doi.org/10.1007/978-3-030-91081-5_6 (Nov. 17–20, 2021) ("Hochman Paper"), at 2-3.

[34] The European Union defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject')." General Data Protection Regulation, Article 4. For an analysis of the use of this term in the European Union, see Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 Calif. L. Rev. 887, 882–87 (2014).

31. Mr. Hochman opines that the categories of Data at Issue in this case automatically constitute PII once they reach the 33-bit (or 29) threshold, a conclusion that he reaches without contextual analysis of Google's actual data processing practices and stated policies.[35] Mr. Hochman appears to believe that because the Data at Issue is complex enough that it could ***theoretically*** distinguish among four billion individuals, that is enough to render the Data at Issue PI or PII irrespective of any other factors, including whether Google takes steps to prevent such linking. But American information privacy standards do not support such an interpretation. On the contrary, these standards make clear that a contextual approach is required to classify the Data at Issue.

32. The critical flaw in Mr. Hochman's approach is that it considers only a high level abstraction, namely the "amount of information"[36] theoretically available to Google and whether it is more or less than 29-bits in the U.S. (or 33-bits globally). This is not the correct methodology to apply in the circumstances of deciding a class certification.

33. Mr. Hochman simply considers how much data to which Google can gain access, and not what measures it may internally take to restrict, limit, or channel access to such data and the linking of that information. As a consequence, Mr. Hochman fails to consider the important issue of whether the Data at Issue could reasonably be linked to an individual in the real world, or whether impediments, including internal protocols or processes, are in place to stop such linkage.

34. Put differently, Mr. Hochman presents a *theoretical* model, and one which may be highly useful for certain experiments in the world of information theory, but fails to consider the kinds of questions on which information privacy standards typically focus. For example, Mr.

[35] Hochman ¶¶ 231-233.

[36] Hochman ¶¶ 166, 231.

Hochman does not look at whether the company processing the Data at Issue has implemented protocols or processes to *prevent* the Data at Issue from being reasonably linked to an individual. In the United States, such measures are a key factor when classifying data. Another common question in U.S. information privacy standards is whether there is a low, moderate, or high probability that the Data at Issue could be linked to an individual.[37] Because Mr. Hochman's approach ignores these important practical considerations, it is contrary to current American information privacy principles.

B. Mr. Hochman's Opinions On PI, PII, And Identifying Information Are Contrary To Information Privacy Standards In The United States.

35. Mr. Hochman's theory of PI, PII, and identifying information is contrary to at least the following: (1) guidance from the Federal Trade Commission (FTC Guidance), (2) the ALI Data Privacy Principles, and (3) the California Consumer Privacy Act (CCPA). I draw on these three frameworks to illustrate the emerging center of gravity regarding the identifiability of data. These three frameworks are not referenced to indicate any conclusion regarding Google's ultimate legal obligations in this case, but simply to show that Mr. Hochman's theory of personal information conflicts with prevailing U.S. information privacy standards.

36. Even beyond the three comparisons I make below (*i.e.*, to FTC Guidance, ALI principles, and the CCPA), **the concepts of PI, PII, and "identifying information" in the United States are generally limited to instances where data refers to an *identified* individual.**[38] I have explored this point in a series of articles I have written with Professor Daniel Solove, the John

[37] *Infra* ¶¶ 46-50, App. C.

[38] Paul M. Schwartz & Daniel Solove, *Reconciling Personal Information in the United States and European Union*, 102 Calif. L. Rev. 877, 891 (2014) (emphasis in the original).

Marshall Harlan Research Professor of Law at George Washington Law School.[39] The definition of personal information functions as an "on" switch for the application of information privacy law. Without the presence of personal information, the information privacy law regime generally does not apply. For example, **it is not customary to extend legal requirements to de-identified information.** As Professor Solove and I have written: "These laws share the same fundamental assumption—that in the absence of PII, there is no privacy right."[40]

37. Moreover, a key challenge is that regulatory regimes sometimes treated identified and identifiable information the same. As Professor Solove and I wrote in a 2011 N.Y.U. Law Review article, **"whether information is identifiable to a person will depend upon context and cannot be determined *a priori*."**[41]

i. FTC Privacy Framework And Guidance.

38. Before the FTC's 2012 Report, there was a dearth of federal guidance on when data should be considered identifiable to an individual. The 2012 FTC guidance "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers" addressed this gap.[42] In the Staff Report, the Commission considered commenters' concerns that,

---

[39] *See id.*; Paul M. Schwartz & Daniel J. Solove, *Defining "Personal Data" in the European Union and U.S.*, 13 Priv. & Sec. L. Rep. 1581 (Sept. 15, 2014); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814 (2011). For a comparative perspective on this issue, *see* Paul M. Schwartz, *"Personenbezogene Daten" aus internationaler Perspektive*, Zeitschrift für Datenschutz 97 (3/2011) ("Personal-specific Data" from an International Perspective).

[40] Schwartz & Solove, *Reconciling Personal Information in the United States and European Union*, supra note 34, at 879. *See also,* Paul M. Schwartz & Daniel J. Solove, *The PII Problem, supra* note 5*,* at 1877–83) (developing a model based on United States and EU law that frees aggregate data and "high-level information" from information privacy obligations).

[41] Schwartz & Solove, *The PII Problem*, supra note 5, at 1836.

[42] Federal Trade Commission (F.T.C.) Report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers" (March 26, 2012).

with improvements in technology and the ubiquity of public information, more and more data could be "reasonably linked" to a consumer and that the proposed framework provided less incentive for a business to try to de-identify and prevent identification of the data it maintains. To address this challenge, the FTC Staff Report provided clarification to "give companies an incentive to collect and use data in a form that makes it less likely the data will be linked to a particular consumer or device, thereby promoting privacy."[43] The FTC Staff clarified that data is not "reasonably linkable" to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.

39. According to the FTC Report, a company must take "reasonable measures" to ensure that the data is de-identified.[44] The FTC staff stated that, "[c]onsistent with the Commission's approach in its data security cases, what qualifies as a reasonable level of justified confidence depends upon the particular circumstances, including the available methods and technologies."[45] The FTC Staff subsequently also recommended "that the definition of PII only include information that is 'reasonably' linkable to an individual."[46]

40. Additionally, the nature of data and the purposes for which it will be used are also relevant to a determination of whether data is de-identified. Thus, for example, whether or how a company publicly releases personal data affects whether the steps it has taken to de-identify data

[43] *Id*. at 22.

[44] *Id*. at 21.

[45] *Id.*

[46] In the Matter of Protecting the Privacy of Customers of Broadband & Other Telecommunications Services, WC Docket No. 16-106, Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission (May 27, 2016), https://perma.cc/2EJZ-ENW8.

are considered reasonable. Moreover, according to the FTC, there is no absolute standard for de-identification. Rather, companies are to take reasonable steps to ensure that data is de-identified. Depending on the circumstances, a variety of technical approaches to de-identification may be reasonable, such as deletion or obfuscation (*e.g.*, hashing) of data fields, the addition of sufficient "noise" to data, statistical sampling, or the use of aggregate or synthetic data.[47] In its 2012 Guidance, the Commission also encouraged companies and researchers to continue innovating in the development and evaluation of new and better approaches to de-identification.

41. Mr. Hochman's approach is contrary to the FTC guidance because it fails to consider whether Google (1) takes reasonable measures to ensure that the Data at Issue is de-identified; (2) publicly commits not to try to re-identify the Data at Issue; and (3) contractually prohibits downstream recipients from trying to re-identify the Data at Issue.

ii. ALI Data Privacy Principles.

42. As noted above at Paragraph 10, the ALI was established in 1932 to promote the clarification and simplification of United States law and its adaptation to changing times. The ALI's Data Privacy project began in 2012, and concluded with formal approval by ALI members at their annual meeting in 2019. Following final editorial work, the ALI published the Principles of Data Privacy Law in 2020.[48]

43. As also indicated above at Paragraph 10, I served as a co-reporter on the Data Privacy Principles project and am therefore familiar with it. It is important to note, however, that the Principles reflect the views of the entire ALI, and not merely my views and those of my co-reporter, Professor Solove. The Privacy Principles project constitutes the ALI's judgment

[47] F.T.C. Report, "Protecting Consumer Privacy," supra note 5, at 21.

[48] ALI Data Privacy Principles § 1 (Am. L. Inst. 2020).

regarding U.S. information privacy standards. The Principles were created by an advisory group, the Members Consultative Group; the Council of the ALI; and the many ALI members who contributed to this project during its seven-year process. Moreover, as noted above, the ALI membership formally voted to approve the project, and did so by unanimous voice vote.

44. The ALI Data Privacy Principles contain concepts regarding responsibilities and obligations in the collection and use of personal data—ones that are in accordance with foundational elements of the U.S. approach to information privacy. The ALI Principles are designed to show the coherence of existing law and serve as a framework for industry-specific codes and data privacy model codes.[49] The ALI Principles set forth a series of responsibilities for those collecting or using personal data as well as a set of rights that individuals have regarding their personal information.

45. The ALI Data Privacy Principles define "personal data" as "any data that is identified or identifiable to a specific living individual."[50] As the Principles state:

> [I]t is impractical and undesirable to regulate data when the risk of identification is low. For example, personal data that has been properly de-identified and aggregated can be of great value to research and the advancement of knowledge. For that reason, the Data Privacy Principles are inapplicable to de-identified and aggregated data. When a low risk of identification exists, an application of the Data Privacy Principles would impose costs, burdens, and restrictions on the use of that data that far exceeded any benefit.[51]

46. Further, and according to the Data Privacy Principles, data is "identified" when "it is directly linked to a specific natural person, or when there is a *high probability* that it could be

[49] *Id.* at § 1, Introductory Note.

[50] *Id.* at § 2, Definitions (b).

[51] *Id.* § 2, Comment c.

linked to a specific person."[52] Identified data is personal data under the Data Privacy Principles and is subject to all relevant ALI Principles.

47. Data is "identifiable" when "there is a *moderate probability* that [data] could be linked to a specific natural person by the intended recipient(s) or by others reasonably foreseeable to have access to the data."[53] Under the Data Privacy Principles, identifiable data is subject to some of the ALI Principles but exempt from others.

48. Data is "nonidentifiable" when "there is a *low probability* that it could be linked to a specific natural person."[54] Under the ALI Principles, such data is not personal data.[55]

49. The identifiability of data is not to be determined as an abstract or fixed matter. For example, computer scientists can develop new techniques to link personal data to specific individuals.[56] Accordingly, the ALI Data Privacy Principles propose that the identifiability of data is best viewed as a spectrum of high, moderate, and low categories relating to probabilities and actual practices, instead of black-or-white categories.[57]

50. Mr. Hochman's bright-line, 29-bit definition of PII approach is inconsistent with these ALI principles because it fails to consider the probability that the specific Data at Issue could be linked to a specific natural person, or whether Google is taking specific steps to keep the Data at Issue from being linked to a specific natural person.

---

[52] *Id.* § 2, Definitions (b)(1) (emphasis added).

[53] *Id.* § 2, Definitions (b)(2) (emphasis added).

[54] *Id.* § 2, Definitions (b)(3) (emphasis added).

[55] *Id.*

[56] *Id.* § 2, Comment (c).

[57] *Id.*

iii. CCPA's Definitions Of "Personal Information".

51. Mr. Hochman's approach is fundamentally inconsistent with both definitions of PI used in the CCPA. By its terms, the CCPA limits its two definitions of "personal information" to the relevant portions of the statute. CCPA § 1798.140(v)(1) states that its definition of "[p]ersonal information" is made only "[f]or purposes of this title." Similarly, CCPA § 1798.81.5(d)(1) defines "[p]ersonal information" only "[f]or purposes of this section." Neither provision purports to define "personal information" for purposes of California law more broadly. Nor do these provisions purport to define the term "personal information" for purposes of interpreting the privacy policies of entities operating in California.

52. The first definition of PI in CCPA § 1798.140(*o*)(1)—which plaintiffs cite in their Complaint[58]—applies to the part of the CCPA that relies on actions by the California Attorney General for its enforcement,[59] and under which there is no private right of action for consumers. The California legislature considered—and rejected—a private right of action for any violation of

[58] TAC ¶ 155 ("the Data collected from users in "private browsing mode" qualifies as "personal information" that is protected by the CCPA. Cal. Civ. Code § 1798.140(o).").

[59] Cal. Civ. Code § 1798.155(b) ("The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General."). As of July 1, 2023, a new regulatory authority, the California Privacy Protection Agency, will have authority to bring administrative actions to enforce certain provisions of the CCPA, and the California Attorney General's Office will retain its authority to enforce the CCPA.

the CCPA.[60] Instead, the legislature cabined the private right of action to a narrow definition of personal information.[61]

53. The CCPA uses a second and separate definition of "personal information" (§ 1798.81.5(d)(1)) in a part of the statute that *does* provide a private right of action for consumers. The private right of action concerns the situation of a data breach. This section protects an individual "whose nonencrypted or nonredacted *personal information* … is subject to an *unauthorized access* and exfiltration, *theft*, or *disclosure* as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action."[62]

54. Where the CCPA provides a private right of action to consumers, that is, for certain cases of a data breach, it incorporates the definition of PI "as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5."[63] For this part of the CCPA, "Personal information" means:

> (A) An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social security number. (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv)

[60] In February 2019, California Attorney General Xavier Becerra and Senator Hannah-Beth Jackson introduced a proposed amendment to the CCPA that would have allowed consumers to bring a private right of action for any violation of the CCPA. *California Consumer Privacy Act of 2018: Consumer Remedies*, CA Sen. Bill. 561 (2019).

[61] *See* Christina H. Kroll, CCPA: The California Senate is Not Ready to Expand the Consumer Right of Action Proskauer Priv. L. Blog (May 17, 2019), https://perma.cc/699Z-QENL.

[62] Cal. Civ. Code § 1798.150(a)(1) (West 2018) (emphasis added).

[63] *Id.*

> Medical information. (v) Health insurance information. (vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.[64]

Mr. Hochman fails to consider whether the Data at Issue in this case would be PI under this CCPA definition. According to Mr. Hochman's descriptions of the Data at Issue in this case,[65] however, it appears that none of it falls under this CCPA definition of PI. The Data at Issue is URLs, IPs, and cookies not associated with a Google Account. None of this information is PI under this definition of the CCPA.

55. Mr. Hochman's approach is also contrary to the first definition of PI in the CCPA:

> Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.[66]

The statute then enumerates categories of information that are PI if they are reasonably capable of being linked to a particular consumer, including:

- "(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers."[67]
- "(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement."[68]

---

[64] Cal. Civ. Code § 1798.81.5(d)(1) (West 2018).

[65] Hochman ¶ 99 ("URLs, IP addresses, user agent, referer").

[66] Cal. Civ. Code § 1798.140(*o*)(1).

[67] *Id.*

[68] *Id.*

56. The plain language establishes that an "online identifier," "internet protocol address," "browsing history," or "search history" are "personal information" under this section of the CCPA only if they can be *reasonably linked* to a particular consumer or household. But, if a particular "online identifier," "internet protocol address," "browsing history," and "search history" cannot be reasonably linked to a particular consumer or household then it is not "personal information." Here, too, the CCPA follows the same approach we see in the other information privacy standards surveyed, namely, the FTC Privacy Framework and Guidance and the ALI Data Privacy Principles.

57. In addition, the CCPA does not apply to and expressly excludes "deidentified" information from the scope of its coverage.[69] The CCPA defines the term with care in Section 1798.140(h): "'Deidentified' means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a *particular consumer*, provided that a business that uses deidentified information:

> (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
>
> (2) Has implemented business processes that specifically prohibit reidentification of the information.
>
> (3) Has implemented business processes to prevent inadvertent release of deidentified information.
>
> (4) Makes no attempt to reidentify the information."

58. Moreover, the CCPA provides a means for a business, such as Google, to process data in a manner that results in it no longer being linked to a particular consumer or household.

[69] Cal. Civ. Code § 1798.145(a) ("The obligations imposed on businesses by this title shall not restrict a business' ability to…(5)[c]ollect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information."); Cal. Civ. Code, §1798.140(o)(3) ("Personal information" does not include consumer information that is deidentified or aggregate consumer information.").

The CCPA defines "pseudonymize" or "pseudonymization" as "the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer."[70] Therefore, even if specific information could reasonably be linked to an individual when a business first receives it, the CCPA provides a path under which a business can process data to prevent it from being linked to a particular consumer.

59. Thus, the CCPA's definition of "personal information" considers whether data is reasonably linkable (or whether it has undergone pseudonymization) and how a business processes data. Mr. Hochman's theory is inconsistent with the CCPA's definition of "personal information."

60. The California Privacy Rights Act (CPRA), also known as Proposition 24 (and sometimes referred to as CCPA 2.0), is a ballot measure that was approved by California voters on November 3, 2020. The CPRA amends the provisions of the CCPA of 2018. While the CPRA took effect on December 16, 2020, most of the provisions revising the CCPA only become "operative" on January 1, 2023.

61. There are two pertinent CPRA amendments in relation to personal information in the context of these reports. *First,* the CPRA narrows a wide range of the obligations imposed on businesses by making clear that they "shall not apply to Household data."[71] These narrowed obligations are found in the following sections: 1798.105 (consumers' rights to delete personal information), 1798.106 (consumers' rights to correct inaccurate personal information), 1798.110

[70] Cal. Civ. Code § 1798.140(r).

[71] Cal. Civ. Code § 1798.145(p).

(consumers' right to know what personal information is being collected), and 1798.115 (consumers' right to know what personal information is sold or shared and to whom).

62. *Second*, the CPRA seeks to encourage businesses to keep information in the least or in a lesser identifiable form. It incentivizes such behavior by freeing these enterprises from certain obligations. In pertinent part, it states, "[t]his title shall not be construed to require a business, service provider, or contractor to:

> (1) Reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.
>
> (2) Retain any personal information about a consumer if, in the ordinary course of business that information about the consumer would not be retained.
>
> (3) Maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.[72]

If companies maintain non-PII, for example, the CPRA exempts them from reidentifying such information, or retaining it, or keeping it in a fashion that will allow it to be used to respond to an individual's request to access their information.

63. Mr. Hochman does not take these CPRA amendments into consideration. This gap in his opinion further indicates that his opinions are contrary to U.S. privacy standards.

V. Opinion # 2: Mr. Schneier's Opinions On PI, PII, And Identifying Information Are Similarly Defective And Also Suffer From Additional Deficiencies Due To An Over-Inclusive Framework Where Virtually Any Data Can Be Deemed PII.

64. For the reasons stated above, Mr. Schneier's report suffers from the same deficiencies as Mr. Hochman's report, including (i) a failure to draw on U.S. information standards governing PII, PI, and identifying information; (ii) an absence of acknowledgment that business practices, policies and procedures affect the categorization of information that is identifying and

[72] Cal. Civ. Code § 1798.145(j).

non-identifying. In addition, Mr. Schneier's report suffers from additional shortcomings resulting from his broad and amorphous conception of PI and PII, which would result in a vastly over-inclusive and impractical privacy framework.

65. In contrast to Mr. Hochman, Mr. Schneier offers a broader definition of PI that, according to him, "focus[es] not only on how information is used but how information could be used (*e.g.*, 'can be used,' 'could reasonably be linked')."[73] In considering how information could be used, however, Mr. Schneier does not look at actual Google practices that are in place to restrict its abilities and possibilities to link data. Mr. Schneier cites to one of the California Consumer Privacy Act's definitions of "personal information" and states that such definition is consistent "with [his] understanding as a technologist and with common usage in the field of privacy and security":

> [I]nformation that identifies, relates to, or ***could reasonably be linked with you*** or your household. For example, it could include your name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about your preferences and characteristics.[74]

66. As explained above, (i) the CCPA's concept of "could reasonably be linked" calls for contextual analysis that includes an examination of a company's practices and policies; and (ii) the CCPA recognizes important categories of de-identified data and pseudonymous data.

67. In an effort to suggest it is not possible to maintain a distinction between PII and non-PII, Mr. Schneier cites to the Code of Federal Regulations definition of PII:

> [I]nformation that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and

[73] Schneier ¶ 82.

[74] Schneier ¶ 81 (emphasis added).

> university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. […][***N]on-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available [non-PII] information, could be used to identify an individual***.[75]

In this part of his opinion, Mr. Schneier cites a definition of PII that comes from Title 2 of the CFR and specifically refers to "Grants and Agreements," a topic unrelated to the issue here. In fact, PII is only referenced once in Title 2 and only in the context of restrictions on public access to records.[76]

> No Federal awarding agency may place restrictions on the non-Federal entity that limit public access to the records of the non-Federal entity pertinent to a Federal award, except for protected **personally identifiable information (PII)** or when the Federal awarding agency can demonstrate that such records will be kept confidential and would have been exempted from disclosure pursuant to the Freedom of Information Act (5 U.S.C. 552) or controlled unclassified information pursuant to Executive Order 13556 if the records had belonged to the Federal awarding agency.[77]

68. Even the website Mr. Schneier used, which allows individuals to click on the term PII through the applicable language in 2 CFR § 200.338, states:

> These are the definitions for terms used in this part. **Different definitions may be found in Federal statutes or regulations that apply more specifically to particular programs or activities.** These definitions could be supplemented by additional instructional information provided in government wide standard information collections. For purposes of this part, the following definitions apply[.][78]

---

[75] Schneier ¶ 80 *citing* 2 CFR § 200.79.

[76] 2 CFR § 200.79, https://perma.cc/P9HC-XF2U.

[77] 2 CFR § 200.338, (emphasis added) https://perma.cc/8E4S-2XMY.

[78] 2 CFR § 200.1 (emphasis added) (limiting the scope of 2 CFR § 200.338), https://perma.cc/U9C2-UVVL.

69. In his report, Mr. Schneier treats "identifying information" in a sweeping and tautological fashion as information that identifies individual users. For example, Mr. Schneier writes that "records purportedly stripped of ***identifying information*** could nonetheless be combined with other data in a manner that enabled patients to be personally identified."[79]

70. At a high level, Mr. Schneier offers a totalizing theory in which data is never truly de-identified because it can always be re-identified. This methodology is contrary to U.S. information privacy standards which (a) recognize that data can be de-identified, and (b) place anonymous data outside its scope of protections.

71. Mr. Schneier further states:

> And even if Google is not building user profiles across signed-in and signed-out data, Google's decision to collect and log this data creates the potential for data to be joined in this way. For example, Google's storage of unique identifiers and IP addresses together in logs introduces a risk that data from a users' private browsing will be joined with a user's signed-in data.[80]

This statement is one example of Mr. Schneier being at odds with U.S. information privacy standards, which consider the probability that data will be linked to an individual.

72. In particular, it is essential under these standards to consider policies and practices that Google has adopted to limit its capabilities and latitude to link information.

73. Indeed, Mr. Schneier's approach would have grave implications for these information privacy standards. By considering theoretical and abstract possibilities sufficient to make data into PII, Mr. Schneier would move these standards beyond their current concept of PII. His approach would undercut the current means of establishing coherent boundaries on necessary

[79] Schneier ¶ 224 (emphasis added).

[80] Schneier ¶ 205.

regulation.[81] As a concept, PII helps to set limits on the scope of privacy law.[82] As Daniel Solove and I have written, "In a world overflowing with information, the law cannot possibly regulate all of it."[83]

74. The risk of having too broad or too abstract a definition of PII is to permit an expansion of regulation to a nearly infinite array of information, including practically every piece of statistical or demographic data.[84] Such an expansion would be highly problematic. To again reference my work with Daniel Solove, a concept of PII that looks to the context of data use has a number of positive benefits. First, by drawing a line between PII and non-PII, it permits society to reap the benefits of large data sets, which "play an important role in research, health care, data security, and the dissemination of knowledge generally."[85] Second, drawing a line between PII and non-PII based on the practices of a data processing entity creates an incentive for collecting and maintaining information in the least identifiable form. As Professor Solove and I argue, it can encourage companies to "invest in technologies that truly make identification of personal data less likely."[86] Finally, by looking to the context of data use, one promotes privacy by incentivizing the use of non-PII. Consider a regulatory system that required full access rights for individuals even for de-identified data that a company had pledged to maintain as non-PII, or when there was a theoretical, low probability of re-identification of non-PII. In requiring that this information be

---

[81] Paul M. Schwartz & Daniel J. Solove *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814, 1836–1848 (2011).

[82] *Id.* at 1866.

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] *Id.* at 1887.

maintained so it would always be transformable into PII, the critical privacy principle of minimization of personal data would be undercut.

VI. Opinion # 3: Mr. Hochman And Mr. Schneier Have Classified The Data At Issue Incorrectly.

75. In this section, I evaluate the Data at Issue using the frameworks that Mr. Hochman and Mr. Schneier have set forth; the U.S. information privacy standards expressed in (A) the FTC Guidance (B) the ALI Principles and (C) the CCPA; and (D) Google policies and practices. *See supra* § IV.B. In my opinion, the conclusions that Mr. Hochman and Mr. Schneier reach that the Data at Issue is PI, PII, or identifying information is fundamentally flawed. Had they applied the correct analysis based on governing U.S. privacy standards and Google policies and procedures, they would have been obliged to conclude that the Data at Issue is not personally identifying; that there is a low probability of Google's identification of users; and that the Data at Issue is likely to be exempt from data subject access rights under current U.S. information privacy standards.

A. Mr. Hochman And Mr. Schneier Fail To Take Into Account Google's Policies And Procedures Related To Classifying The Data At Issue.

76. For technical descriptions of the Data at Issue, I am relying on the report of computer scientist Dr. Konstantinos Psounis, and in particular his opinion that the Data at Issue is not associated with a user's Google Account and the Data at Issue is stored in an orphaned and unidentified state.[87]

77. An analysis of Google's policies and guidelines demonstrates the presence of strong privacy protections designed to prevent such Data at Issue from being identified and linked to a particular consumer, or a user's Google Account. Neither Mr. Hochman's categorical approach nor Mr. Schneier's amorphous and open-ended framework take into account Google's policies and

[87] Expert Report of Konstantinos Psounis, PH.D. § III.A.1-2.

guidelines regarding data. Their perspectives are faulty because, as explained above, the steps a company takes to process data to prevent it from being reasonably linked to an identified individual are a key factor in determining its status under relevant information privacy standards. In my opinion, Google's existing policies and guidelines support the conclusion that the Data at Issue is neither PII nor PI. Mr. Hochman does not establish that Google links the Data at Issue with a Google Account; rather, he merely speculates that Google *could* join the Data at Issue with an individual's Google Account. He also does not consider the *likelihood* that this would ever occur and the existence of Google safeguard to prevent such joining of data.

78. In this section, I respond to Mr. Hochman's and Mr. Schneier's Expert Opinions by examining Google's relevant policies. Google has implemented policies and taken certain steps regarding the Data at Issue, namely information that is *not* associated with a user's Google Account. These steps seek to ensure that such information is neither linked nor reasonably linkable to a specific individual by Google. Moreover, Google's Anti-Fingerprinting Policy prevents certain steps by Google employees that might increase the identifiability of certain information. These policies are described more fully in the sections that follow.

79. The information privacy standards that this Expert Opinion examined above, namely the ALI Data Privacy Principles, the FTC Staff Report, and the CCPA, underscore the relevance of Google's policies and practices. Specifically, these standards require consideration of what companies permit and do not permit with personal data. As a consequence, Google's Privacy Policy, Data Categorization Guidelines, and Anti-Fingerprinting policy are highly significant documents for classifying the Data at Issue.

80. To be clear, I am not analyzing whether it is theoretically possible for Google, or a rogue Google employee, to identify an individual using non-Google Account linked data through

"finger-printing." Whether data is "theoretically linkable" to an individual is not a standard for determining whether data is PI or PII. Moreover, my understanding is that "finger-printing" would be in violation of Google's policies and also would require circumvention of Google's technical barriers that apply to the segregated repositories that Google uses to store data.

i. Google's Privacy Policy.

81. The Google Privacy Policy defines "personal information" as "information that you provide to us which personally identifies you, such as your *name*, *email address*, or *billing information*, or other data that can be *reasonably linked to such information by Google*, such as information *we associate with your Google Account*."[88] Under this definition, apart from enumerated categories of information that personally identify an individual—*i.e.* name, email address, billing information—data is "personal information" only if Google can reasonably link it to an identified individual. Thus, plaintiffs' categorical approach of defining PI as *always* including the Data at Issue is inconsistent with Google's own Privacy Policy definition. Under that definition of "personal information," the Data at Issue *does* fall in this category when Google associates it with the user's Google Account.

82. When Google does not associate the Data at Issue with a user's Google Account, and takes steps to ensure the data cannot reasonably be linked to information that personally identifies an individual—*e.g.*, when Google implements protocols and policies to prevent such linking—as is the case here, the Data at Issue is not "personal information" under the Google Privacy Policy. Whether, when, and which data is reasonably linkable by Google to information

[88] Google Privacy & Terms, Privacy Policy Key Terms (Last Accessed Jun. 3, 2022), https://perma.cc/524M-5UH2 (emphases added).

that personally identifies an individual depends on Google's practices and policies (namely, those discussed in the three sections that follow).

ii. Google's Data Categorization Guidelines.

83. Beyond the Google Privacy Policy, another important privacy instrument in use at Google is its Data Categorization Guidelines.[89] This document defines "User Data" as [redacted][90] The Google Data Categorization Guidelines further state, [redacted][91] These Google Guidelines define them as follows:

[redacted]

[89] Data Categorization Guidelines, GOOG-CABR-04400013.

[90] *Id.*

[91] *Id.* at -014.

[redacted]

[redacted]

84. Google Guidelines also state, [redacted]

[redacted][93]

85. Google's Data Categorization Guidelines applies the following basic guidelines to categorizing data as identifiable/PII:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[92] *Id.* at -014-15.

[93] *Id.* at -015 (emphasis added).

[94] *Id.* at -014.

86. In my opinion, Google's data categorization guidelines reflect the U.S. information privacy standards discussed in this report. An important aspect of how these guidelines incorporate these standards is their incorporation of a benchmark of whether data is "reasonably likely" to identify any person.

iii. Google's Anti-Fingerprinting Policy.

87. Since January 2015, Google has maintained an official Internal Privacy Policy on the use of device/app/browser fingerprinting and immutable identifiers.[95] Google's anti-fingerprinting policy prohibits the use of [redacted][96] As a consequence of this anti-fingerprinting policy, Google employees are prohibited from using specific categories of the Data at Issue—*i.e.*, IP address, User-Agent, X-Client-Data Header[97]—to identify and track a browser or user across distinct transactions.

88. Google's platform policies make explicitly clear that Google's platform products—which include "Authorized Buyers, Campaign Manager 360, Google Ad Manager 360, Google Ad

[95] *See* Device/App/Browser Fingerprinting and Immutable Identifiers Policy, GOOG-CALH-00027147.

[96] *Id.* (Google's anti-fingerprinting policy explicitly lists "IP address" as an example of an attribute that should be considered unique).

[97] Decl. of Alexei Svitkine ¶ 4, Dkt. 112-5 ("The X-Client-Data header is designed to have low entropy and is not uniquely identifying. Indeed, the header assigned to a particular instance of Chrome is based on a random number from 0 to 7999 precisely to prevent it from being used to uniquely identify the user or browser. In practical terms, this means that the XClient-Data header for any particular instance of Chrome is identical to the header assigned to many other Chrome users.").

Manager, Search Ads 360, and Display & Video 360"[98]—must not be used "to identify users or facilitate the merging of personally-identifiable information with information previously collected as non-personally identifiable information without robust notice of, and the user's prior affirmative (*i.e.* opt-in) consent to, that identification or merger."[99] Irrespective of users' consent, there must be no attempt to disaggregate data that Google reports in aggregate.[100] Furthermore, to "protect user privacy, Google policies mandate that no data be passed to Google [by Google Analytics customers] that Google could use or recognize as personally identifiable information (PII)."[101]

89. Google's anti-fingerprinting policy is a function of its strong policy against anti-fingerprinting. Google has publicly stated that "Google doesn't use fingerprinting for ads personalization because it doesn't allow reasonable user control and transparency. Nor do we let others bring fingerprinting data into our advertising products."[102] Google has publicly confirmed it will "continue to disallow fingerprinting on its products and via its platforms, as per its long-standing policies."[103]

90. Therefore, in the context of fingerprinting, Google has a stated policy that expressly prohibits the use of certain of the Data at Issue to identify users. Moreover, Google publicly commits to not using the Data at Issue to identify users. Finally, Google contractually prohibits

---

[98] *Platforms Program Policies*, Google Help Center, (Last Updated Apr. 1, 2022), https://perma.cc/7D86-XR54.

[99] *Id.*

[100] *Id.*

[101] Best Practices to Avoid Sending Personally Identifiable Information (PII), Analytics Help Center, (2021), https://perma.cc/L7LG-CG7W.

[102] Prabhakar Raghavan, Raising the Bar on Transparency, Choice and Control in Digital Advertising, (May 7, 2019), Google Ads & Commerce Blog, https://perma.cc/HQH3-PPBE; *see also* GOOG-CALH-00029480.

[103] GBO Comms Document, GOOG-CABR-04310004.

other companies from identifying users as well. All of these factors must be taken into consideration when classifying the Data at Issue.

iv. Google's Policies Against Re-Identifying Individuals.

91. Google's Log Data Usage Rules contain a series of prohibitions for Google employees that bear directly on Mr. Hochman's Expert Opinions. Specifically, Google's User Data Anonymization Policy prohibits Google employees from re-identifying any individual from Anonymous or Pseudonymous data.[104] [redacted][107]

92. Google's 2020 Log Data Usage Rules include a relevant section on re-identification of logs data.[108] I have reproduced it here:

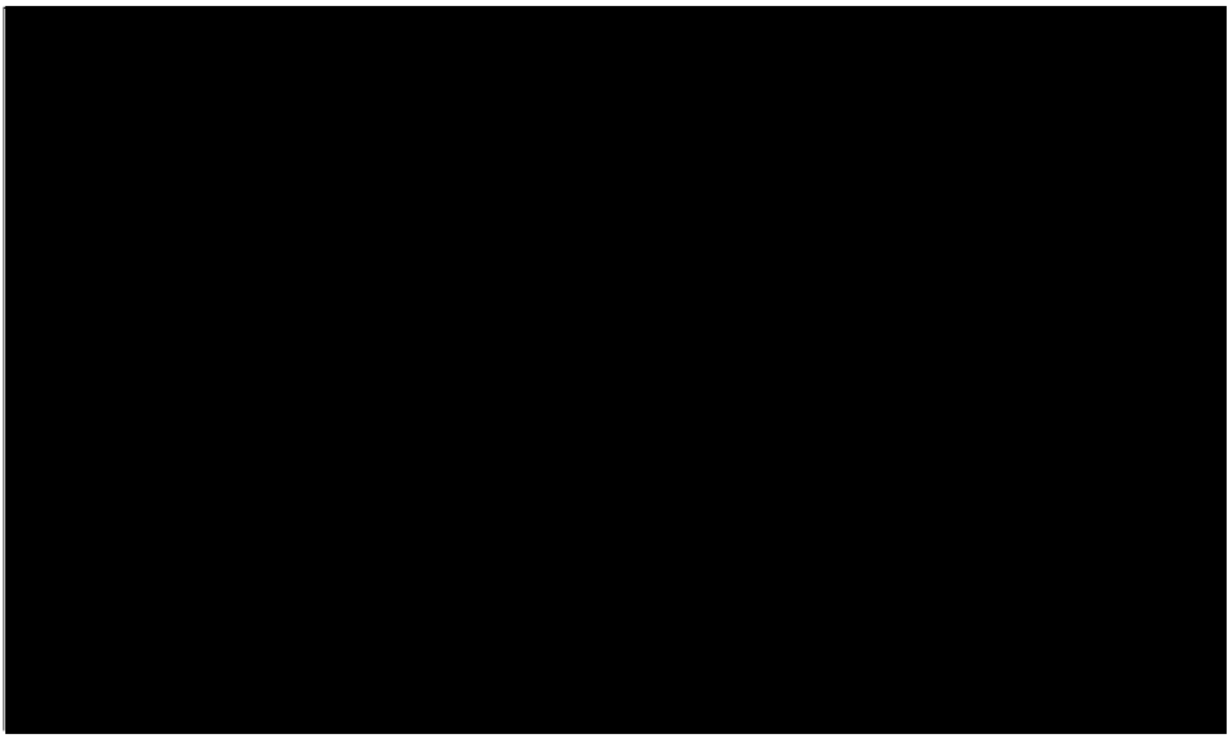
[104] Log Data Usage Rules, GOOG-BRWN-00029004 at -006.

[105] *Id.*

[106] *Id.*

[107] *Id. See also* Google Factbase: Ads Data Policies and Statements, GOOG-CABR-0460448

[108] *See* GOOG-BRWN-00029004; *see also* Monsees Dep. (30b6) at 311:12-313:12, Apr. 9, 2021, *Calhoun v. Google*, 5:20-cv-05146-LHK.



GOOG-BRWN-00029004 at -006.

93. In addition, as Google employee David Monsees explained in a declaration filed in the *Calhoun v. Google* action, Google engages in the following practices to ensure that pseudonymous-keyed log data are not used to uniquely identify individual users including: IP address redaction and cookie scrubbing,[109] limiting the access of individual Googlers to either pseudonymous-keyed data sources or Google Account-keyed data sources,[110] prohibiting determinative joins between Google Account-keyed data and pseudonymous-keyed data,[111] avoiding logging specific IDs to prevent an indirect and inadvertent join between Google Account-keyed data and pseudonymous-keyed data,[112] and ensuring that "identifiers such as Biscotti or

[109] Scrubbing Policies for Log Data, GOOG-CALH-00027152.

[110] Ads Cookies, GOOG-CABR-04696282 at -284.

[111] *Id.* at -285.

[112] *Id.*

Zwieback must never be stored with personally-identifying information (PII) such as GAIA IDs [Google Account IDs]."[113]

B. The Data At Issue Is Not Personally Identifying, Has A Low Probability Of Identification, And Is Exempt From Data Subject Access Rights.

i. The Data At Issue Is Not Reasonably Linkable Under FTC Guidance.

94. Both Mr. Hochman and Mr. Schneier fail to consider what qualifies as "reasonably linkable" data under the FTC and what Google does in practice in relation to this FTC guidance. As illustrated in the table below, my analysis of Google's relevant policies and practices shows that Google takes steps to make the Data at Issue not "reasonably linkable" pursuant to the FTC guidance.

#	**FTC Guidance** Data is not "reasonably linkable" to the extent that a company:	**Google Policies and Practices**
1.	"Takes reasonable measures to ensure that the data is de-identified;"	[redacted]
2.	"[P]ublicly commits not to try to re-identify the data; and"	• "Chrome also announced that it will more aggressively restrict

[113] *Id.* at -286. *See also*, Decl. of D. Monsees ¶10, Calhoun v. Google, 5:20-cv-05146-LHK, (Dkt. No. 428-22).

[114] *See supra* § VI.A.iv.

[115] *Id.*

[116] *Id.*

		fingerprinting across the web."[117] ● "[We] will aggressively combat the current techniques for non-cookie based cross-site tracking, such as fingerprinting, cache inspection, link decoration, network tracking and Personally Identifying Information (PII) joins."[118] ● "[W]e're developing techniques to detect and mitigate covert tracking and workarounds by launching new anti-fingerprinting measures to discourage these kinds of deceptive and intrusive techniques."[119] ● "Google doesn't use fingerprinting for ads personalization because it doesn't allow reasonable user control and transparency."[120]
3.	"contractually prohibits downstream recipients from trying to re-identify the data."	● "Nor do we let others bring fingerprinting data into our advertising products."[121] ● "You must not use device fingerprints or locally shared objects (*e.g.*, Flash cookies, Browser Helper Objects, HTML5 local storage) other than HTTP cookies, or user-resettable device identifiers designed for use in measurement or advertising, in connection with Google Analytics."[122] ● "[W]e remind you that our policies prohibit fingerprinting for identification (*e.g.*, Requirements for Third Party Ad Serving), and we require that you adhere to our policies, which can be more restrictive than the TCF v2.0 in some cases, whenever you work with us."[123] ● "Ads may not directly capture any personally-identifiable user information. Personal information includes, but isn't limited to, e-mail addresses, telephone numbers, and credit card numbers.

[117] Prabhakar Raghavan, Raising the Bar on Transparency, Choice and Control in Digital Advertising, (May 7, 2019), Google Ads & Commerce Blog, https://perma.cc/HQH3-PPBE.

[118] *The Privacy Sandbox*, Chromium Blog, https://perma.cc/7GGQ-7YV7 (last accessed Jun. 4, 2022).

[119] Justin Schuh, *Building a more private web: A path towards making third party cookies obsolete*, Chromium Blog, (Jan. 14, 2020), https://perma.cc/8LCF-7N4A.

[120] Prabhakar Raghavan, Raising the Bar on Transparency, Choice and Control in Digital Advertising, (May 7, 2019), Google Ads & Commerce Blog, https://perma.cc/HQH3-PPBE.

[121] *Id.*

[122] *Policy Against Fingerprints and Locally Shared Objects*, Google Analytics Help Center (2022), https://perma.cc/V44X-GEZK.

[123] *Interoperability guidance for vendors working with Google via the IAB TCFv2.0*, Google Ad Manager Help Center (2022), https://perma.cc/EC8S-MVJK.

		No sensitive information can be collected through the ad. You may not associate cookies, web beacons, or other tracking mechanisms with personally-identifiable information (PII) for any purpose or with precise user location for behavior targeting unless the user has knowingly and expressly opted in. (For purposes of this document, PII and precise user location does not include IP addresses.)"[124]

95. Based on comparing Google's practices with its publicly available policies and procedures, it is my opinion that Google, as recommended by the FTC, "[t]akes reasonable measures to ensure that the data is de-identified; publicly commits not to try to re-identify the data; and contractually prohibits downstream recipients from trying to re-identify the data."

ii. Under ALI Principles, There Is A Low Probability That Google Could Link The Data At Issue To A Specific Natural Person.

96. Under the ALI Data Privacy Principles, data is "identified" when "it is directly linked to a specific natural person, or when there is a *high probability* that it could be linked to a specific person."[125] It also explains that data is "'nonidentifiable'" when there is a low probability that it could be linked in to a specific natural person."[126] Such information is not "personal data" under the Data Privacy Principles.[127] Indeed, the Principles establish the idea of "spectrum of probabilities" for defining personal data.[128] As indicated above, both Mr. Hochman and Mr. Schneier fail to adequately consider Google's privacy policies and practices. Due to these policies

[124] *Requirements for third-party ad serving*, Google Advertising Policies Help (2022), https://perma.cc/JP2W-8H7Z.

[125] ALI Data Privacy Principles § 2, Definitions (b)(1) (emphasis added).

[126] *Id.* at (b)(3).

[127] *Id.*

[128] *Id*. at Comment (c).

and practices, there is not a "high probability" that the Data at Issue can be linked to a specific person. Rather, as a result of Google's privacy policies and practices, there is a low probability that the Data at Issue is personal data that is not directly linked to a specific natural person.

iii. The Data At Issue Is Exempt From Certain Breach Notification Requirements, Portability, and Access and Correction Rights.

97. As in defining "personal data," the ALI Data Privacy Principles rely on a contextual approach when it discusses the requirement for data breach notifications. The Principles free data processors from any obligations to notify an affected party of such breaches under circumstances when there is "a low probability" of risk. It states:

> (5) The factors to be considered in determining whether there is a *low probability* that personal data will be compromised include:
>
> > (A) the nature and extent of the personal data involved, including the types of identifiers and the likelihood of reidentification;
> >
> > (B) the identity of the unauthorized person to whom the personal data was disclosed or who used it;
> >
> > (C) whether the personal data was actually acquired or accessed; and
> >
> > (D) the extent to which the risk of compromise of the personal data has been mitigated.
>
> (6) Notification is not required when the personal data was properly encrypted and the encryption keys are not compromised or breached.[129]

98. Crucially, this language indicates that even when personal data is involved in a breach, a critical requirement continues to be a contextual analysis, and one that turns on an evaluation of risk factors.

99. As for a data portability request, it "permits a data subject to control his or her ***personal information*** and can also further consumer choice among enterprises."[130] The idea of

[129] ALI Data Privacy Principles, § 11 Data Security and Data Breach Notification. (emphasis added).

[130] ALI Data Privacy Principles, § 9 Data Portability, Comment (a).

data portability is to allow consumers to request and receive the personal data that one company has collected about them, and then be able to move the data to another company. Importantly, pursuant to ALI Principles, "[i]f only identifiable personal data is maintained about a data subject and if complying with a data portability request would require identifying this personal data, then the data controller **does not have to comply with the data portability request**."[131] Thus, the Data at Issue is exempt from data subject portability interests as defined in the ALI Data Privacy Principles.

100. Finally, there is the matter of access and correction rights. The ALI Principles allow individuals to access their personal data and request corrections of errors. These interests are limited, however, only to identified data. Indeed, the ALI Data Privacy Principles explicitly state, "[a]ccess and correction rights extend under these Principles only to identified data and not identifiable data."[132] Recall that "identifiable data" is information where there is a moderate probability of linkage to a specific person, but that connection has not yet been made. The Principles warn:

> Access and correction rights do not extend to identifiable data because such rights would result in more personal data becoming identified, which would increase risks to the privacy and security of data. Such an interest might also impose excessive compliance costs on data controllers, who would be obligated to carry out onerous searches of their databases for information that was linkable to a specific individual.[133]

The Data at Issue provides a clear illustration of information that is not identified, and, hence, not subject to access and correction interests pursuant to the ALI Data Privacy Principles.

---

[131] *Id.* at § 9(f), Data Portability (emphasis added).

[132] *Id*. at § 8, Comment b.

[133] *Id*.

C. Individualized Determinations Would Be Required In Any Attempt To Establish That The Data At Issue Is PI Or PII.

101. In my opinion, as stated above, the Data at Issue is non-identifying and not PII or PI under U.S. privacy industry standards. Any attempt to show otherwise would necessarily require fact-intensive and individualized inquiries for each Data at Issue and each putative class member. That result follows because whether the Data at Issue has any probability of being reasonably likely to identify a particular class member cannot be uniformly answered as to all class members as the class is currently defined.[134] Such a determination is necessarily a fact-bound one that will turn on the type of data; whether the specific data is pseudonymous or anonymous; and whether Google has processed the specific data to de-identify, pseudonymize, or prevent individual identification.

102. The easiest scenario under which data is likely PI or PII is one that does not apply to this case. Under this scenario Google associates certain data (IP address, user-agent, cookies, and URLs) with a user's Google Account. In that scenario, the Data can be classified as PI under most standards.[135] Specifically, such data is likely to be "identified" information under the ALI Data Privacy principles; it is likely PI under the FTC Guidance; and it is likely PI under one provision of the CCPA, namely § 1798.140(*o*)(1).

103. However, as demonstrated above, Google does not associate the Data at Issue with a user's Google Account. Hence, the determination of whether the data related to a putative class member's browsing is PI or PII necessarily raises a series of complex factual questions. Under the FTC guidance, a determination has to be made on whether the data is "reasonably linkable" to a

[134] TAC ¶ 192. *See also*, TAC ¶ 93 .

[135] I discuss Google's Privacy Policy above in this Expert Opinion. *See supra* § VI.A.i.

consumer or their device.[136] Under the ALI principles, the probability that such data is linked to an identified individual has to be taken into consideration.[137] Similarly, under the CCPA section that plaintiffs cite in their Complaint and Mr. Schneier references (1798.140(*o*)(1)), data is PI if it could reasonably be linked with a particular consumer.[138] Under either of these approaches, whether Data at Issue is non-identifying or has a low probability of identification requires additional individualized fact-intensive determinations for each individual set of data and cannot be made on a classwide basis.

104. To illustrate the above, I briefly discuss two of the types of Data at Issue in this case below.

(a) **IP Address.** The degree to which any given IP address is non-identifying or has a low probability of identification varies and will turn on answers to a number of questions, including: Is the IP address cloaked through a VPN? Is the IP address associated with an individual's home address or is it associated with a place generally open to the public? The latter kind of a location would include a coffee shop that offers wifi, such as a Starbucks. Other issues are relevant to the issue of judging whether an IP address is "personal information." Is the IP address static or

[136] Federal Trade Commission (F.T.C.), Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, at 22 (March 26, 2012).

[137] ALI Data Privacy Principles § 2, Comment c.

[138] *See also*, "The obligations imposed on businesses in Sections 1798.105, 1798.106, 1798.110, and 1798.115 shall not apply to household data." Cal. Civ. Code § 1798.145(p), *AB-2891 California Consumer Privacy Act: exemption*. AB-2891 or the California Privacy Rights Act (CPRA) is a ballot measure (Proposition 24) that was approved by California voters on November 3, 2020 and took effect on December 16, 2020; however, most of the provisions revising the CCPA will become operative by January 1, 2023. The CPRA significantly amends the CCPA, and it is periodically referred to as "CCPA 2.0."

dynamic?[139] Does the IP address identify a device on the internet, or a network of devices? Is the IP address an IPv4 or IPv6 address?[140]

(b) **Cookies.** A different case would involve cookies that contain the user's Google Account information (*e.g.*, cookies that contain a GAIA ID). I am also informed that a Google Account permits a user to either include a real name, or to supply a pseudonym. A Google Account can also include an email address. If Google associates the content of such cookies with a user's Google Account, and if the account includes a person's real name and email address, the content of those cookies is likely PI. However, I am informed that the cookies at issue in this case do *not* contain any GAIA IDs. The degree to which the cookies at issue in this case can reasonably be linked with a particular consumer will vary significantly, and turn on Google's server-side practices and specific cookie attributes, including: Has Google employed measures that prevent data from being reasonably linked to an identified individual? Is the cookie a first or a third party cookie? For how long does the cookie persist on a user's browser? Does the cookie contain a pseudonymous ID?

105. In sum, Mr. Hochman's and Mr. Schneier's assertion that the Data at Issue is PI or PII—regardless of the content of the specific data or the circumstances of how it is stored and processed—is generally inconsistent with American information privacy standards. None of the Data at Issue is associated with a user's Google Account, which means the data is unauthenticated

[139] A dynamic IP address is one that changes frequently.

[140] *See* Psounis Rep. § III.G.1.a.

(*i.e.*, not associated with a specific user's identity), and Google implements policies and technical controls to prevent its re-identification.[141]

***

106. The analyses and opinions in this report are based on the results of my research, my review and analysis of the materials provided to me, my education and training, and my experience on related topics. As additional materials and information become available or if the scope of discovery or the causes of action change in any material way, I reserve the right to amend, supplement, or update my analysis and conclusions.

Paul M. Schwartz
Paul M. Schwartz
June 7, 2022

[141] Psounis Rep. § III.A.; *See also* GOOG-CABR-00073880 at -882 ("Technical controls against inadvertent re-identification . . . include access control for any mapping between pseudonyms and other user identifiers (*e.g.*, mappings that may be used to append to pseudonymous data sets that contain stable identifiers), and anonymization techniques such as generalization of potentially unique data elements.").

APPENDICES

A. Definitions of Personally Identifiable Information

Source	Personally Identifiable Information
Mr. Hochman's Expert Report	"It is my opinion that an IP address, especially when combined with a user-agent string, constitutes personally identifiable information ('PII') because this data can be used to uniquely identify a user with a high probability of success. Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used to deanonymize previously anonymous data is considered PII[.]"[142] "One metric for user identifiability is called entropy, measured in number of bits of data needed to uniquely identify a person. With a little less than 8 billion people on earth, 33 bits of data is needed to uniquely identify a person (2^33 = 8.6 billion). With around 330 million people in the United States, 29 bits of data is more than sufficient to identify a person (2^29 = 537 million)."[143]
Mr. Schneier's Expert Report	"User data encompasses a range of information. Certain forms of personally identifying information—for example, name, address, Social Security number, passport or driver's license number, banking and credit card information—are often collected from users of products and services in the course of establishing accounts."[144] "Personally identifiable information is also generated in the course of using customer accounts. In the case of Internet services, these include highly personal records of users' online activity. Web browsing results in the accumulation of cookies and the creation of logs containing information from that web browsing. Full URLs often incorporate page titles, and therefore do more than just represent a web address; they may also indicate the content of the page."[145]

[142] Hochman Rep. ¶ 105 (internal quotation marks omitted).
[143] *Id.* ¶ 231.
[144] Schneier ¶ 79.
[145] *Id.* ¶ 83.

FTC[146]	FTC staff recommends that the definition of PII only include information that is "reasonably" linkable to an individual.
Google's Contracts and Policies[147]	"Google interprets PII as information that could be used on its own to directly identify, contact, or precisely locate an individual. This includes: • email addresses • mailing addresses • phone numbers • precise locations (such as GPS coordinates - but see the note below) • full names or usernames For example, if you're a publisher whose contract prohibits you from passing PII to Google, the URLs of pages on your website that display ads by Google must not include email addresses, because those URLs would be passed to Google in any ad request. Google has long interpreted its PII prohibition in this way. Note: Certain product's help centers and policies set out the limited means by which certain forms of PII may be sent to Google. For avoidance of doubt, this article does not amend such provisions. So, for example, certain products allow approximate location data to be sent to Google, provided the requirements of the applicable policies are met. Google interprets PII to exclude, for example: • pseudonymous cookie IDs • pseudonymous advertising IDs • IP addresses • other pseudonymous end user identifiers

[146] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, at 18-20 (March 26, 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[147] Understanding PII in Google's Contracts and Policies, Google Help Center, (2021), https://support.google.com/analytics/answer/7686480.

	For instance, if an IP address is sent with an ad request (which will be the case with almost any ad request as a consequence of internet protocols), that transmission will not breach any prohibition on sending PII to Google. Note that data excluded from Google's interpretation of PII may still be considered personal data or personal information under the GDPR, CCPA, and other privacy legislation. This article doesn't affect any contract provisions or policies relating to personal data or personal information under those laws."
U.S. Department of Labor - Guidance on the Protection of Personal Identifiable Information [148]	"Personal Identifiable Information (PII) is defined as: Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (*e.g.*, name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, *i.e.*, indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media."
Code of Federal Regulations - Part 200—Uniform Administrative Requirements, Cost Principles, and Audit	"Personally Identifiable Information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public websites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non–PII can become

[148] U.S. Department of Labor, Guidance on the Protection of Personal Identifiable Information, (last visited Dec. 21, 2021), https://www.dol.gov/general/ppii.

Requirements for Federal Awards [149]	PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual."
NIST Computer Security Resource Center[150] - NIST SP 800-79-2[151] under PII from EGovAct[152]	"Personally Identifiable Information; Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."
NIST Computer Security Resource Center - NIST SP 800-37 Rev. 2[153]	"Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."
NIST Computer Security Resource Center - NISTIR 8053[154] under PII from GAOReport 08-536, NIST SP 800-122[155]	"Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

[149] 2 C.F.R. § 200.1 (2021).
[150] National Institute of Standards and Technology, Glossary: Personally Identifiable Information (PII), (last visited Dec. 21, 2021), https://csrc.nist.gov/glossary/term/personally_identifiable_information.
[151] Ferraiolo, et al., Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI) at 46, (July 2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-79-2.pdf.
[152] E–GOVERNMENT ACT OF 2002, PL 107–347, December 17, 2002, 116 Stat 2899.
[153] *See* Ross, et al., Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy at 1, (December 2018), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (*quoting* Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016).
[154] Simson L. Garfinkel, De-Identification of Personal Information at 42-43, (October 2015), https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.
[155] GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, (May 2008), http://www.gao.gov/new.items/d08536.pdf.

U.S. General Services Administration[156]	"The term 'PII,' as defined in OMB Memorandum M-07-1616 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual."
2180.2 CIO GSA Rules of Behavior for Handling Personally Identifiable Information (PII)[157]	"PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified using information that is linked or linkable to said individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other information to identify a specific individual, could be used to identify an individual (*e.g.*, Social Security Number (SSN), name, date of birth (DOB), home address, personal email)."
US Department of Energy - DOE O 203.2, Mobile Technology Management[158]	"Any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual."
US Department of Energy - DOE O 206.1 Chg1	"Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. PII can include

[156] U.S. General Services Administration, Rules and Policies - Protecting PII - Privacy Act, (Last Reviewed Jan. 12, 2020), https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act.

[157] Beth Anne Killoran, U.S. General Services Administration, 2180.2 CIO GSA Rules of Behavior for Handling Personally Identifiable Information (PII), (Oct. 19, 2019), https://www.gsa.gov/directive/gsa-rules-of-behavior-for-handling-personally-identifiable-information-(pii)- .

[158] Mobile Tech. Mgmt., US DOE 203.2 (May 15, 2014), https://www.energy.gov/sites/default/files/2015/08/f25/o203.2.pdf.

(MinChg), Department of Energy Privacy Program[159]	unique individual identifiers or combinations of identifiers, such as an individual's name, Social Security number, date and place of birth, mother's maiden name, biometric data, etc. The sensitivity of PII increases when combinations of elements increase the ability to identify or target a specific individual. PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual is categorized as High Risk PII. Examples of High Risk PII include, Social Security Numbers (SSNs), biometric records (*e.g.*, fingerprints, DNA, etc.), health and medical information, financial information (*e.g.*, credit card numbers, credit reports, bank account numbers, etc.), and security information (*e.g.*, security clearance information). While all PII must be handled and protected appropriately, High Risk PII must be given greater protection and consideration following a breach because of the increased risk of harm to an individual if it is misused or compromised."
US Department of Energy - DOE O 443.1C, Protection of Human Research Subjects[160]	"Any information collected or maintained about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and any other personal information that is linked or linkable to a specific individual."
Department of Commerce: Office of Privacy and Open Government - Safeguarding Information[161]	"The term personally identifiable information refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in harm, embarrassment, inconvenience, or unfairness to an individual. The following types of PII are considered

[159] Minor Changes to Doe O 206.1, Dep't of Energy Priv. Program, US DOE 206.1 (Nov. 1, 2018), https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder-chg1-minchg/@@images/file.

[160] Prot. of Hum. Rsch. Subjects, US DOE 443.1C at 20 (Nov. 26, 2019). https://www.directives.doe.gov/directives-documents/400-series/0443.1-BOrder-c/@@images/file at 20.

[161] U.S. Dept. of Commerce, Safeguarding Information, (last updated Oct. 1, 2021), https://www.osec.doc.gov/opog/privacy/pii_bii.html.

	sensitive when associated with an individual: Social Security Number (including truncated form), place of birth, date of birth, mother's maiden name, biometric information, medical information (excluding brief references to absences from work), personal financial information, credit card or purchase card account numbers, passport numbers, potentially sensitive employment information (*e.g.*, performance ratings, disciplinary actions, and results of background investigations), criminal history, and any information that may stigmatize or adversely affect an individual. Context of information is important. The same types of information can be sensitive or non-sensitive depending upon the context. For example, a list of names and phone numbers for the Department's softball roster is very different from a list of names and phone numbers for individuals being treated for an infectious disease. If sensitive PII is electronically transmitted, it must be protected by secure methodologies, such as encryption, Public Key Infrastructure, or secure sockets layer. When in doubt, treat PII as sensitive."
US Department of Education[162]	"Personally identifiable information (PII) includes information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information."
Family Educational Rights and Privacy Act Regulations, 34 CFR §99.3[163]	"The term includes, but is not limited to - (a) The student's name; (b) The name of the student's parent or other family members; (c) The address of the student or student's family; (d) A personal identifier, such as the student's social security number, student number, or biometric record; (e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

[162] U.S. Dept. of Education, Protecting Student Privacy, (Last Visited Dec. 21, 2021), https://studentprivacy.ed.gov/content/personally-identifiable-information-pii.

[163] https://www.ecfr.gov/current/title-34/subtitle-A/part-99, (*citing* 20 U.S.C. 1232g, https://www.govinfo.gov/content/pkg/USCODE-2019-title20/pdf/USCODE-2019-title20-chap31-subchapIII-part4-sec1232g.pdf), (Last Visited Dec. 21, 2021).

	(f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates."
California Business and Professions Code §22577(a) - Division 8. Special Business Regulations - Chapter 22. Internet Privacy Requirements [164]	"(a) The term 'personally identifiable information' means individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following: (1) A first and last name. (2) A home or other physical address, including street name and name of a city or town. (3) An e-mail address. (4) A telephone number. (5) A social security number. (6) Any other identifier that permits the physical or online contacting of a specific individual. (7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision."
Penal Code § 530.55, subdivisions (a) and (b) - Title 13. Of Crimes Against Property - Chapter 8. False Personation and Cheats [165]	"(a) For purposes of this chapter, 'person' means a natural person, living or deceased, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity, or any other legal entity. (b) For purposes of this chapter, 'personal identifying information' means any name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license, or identification number, social security number, place of employment, employee identification number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, United States Citizenship and Immigration Services-assigned number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the person, address or routing

[164] California Business and Professions Code §22577(a) https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22577, (Last Visited Jun. 4, 2022).
[165] Cal. Penal Code § 530.55 (West 2007).

	code, telecommunication identifying information or access device, information contained in a birth or death certificate, or credit card number of an individual person, or an equivalent form of identification."
CALJIC 15.61[166]	"The phrase, 'personal identifying information' means the [name, address, telephone number,] [health insurance [identification] number,] [taxpayer identification number,] [school identification number,] [state or federal driver's license number, or identification number,] [social security number,][place of employment,] [employee identification number,] [professional or occupational number][mother's maiden name,] [demand deposit number,] [savings account number,] [checking account number,] [PIN (personal identification number) or password,] [alien identification registration number,] [government passport number,] [date of birth,] [unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image,] [or] [other] [unique physical representation,] [unique electronic data including [information] identification number assigned to the person, address, or routing code,] [telephonic communication identifying information or access device,] [information contained in a birth or death certificate or credit card number of a person, or an equivalent form of identification]. [For the purposes of this section, 'person' means a natural person, [living or deceased] firm, [association,] organization, partnership, business trust, company, corporation, limited liability company or public entity [, or any other legal entity].]"
Song-Beverly Act[167]	"(b) For purposes of this section 'personal identification information,' means information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number."
Video Privacy Protection Act of 1988 (VPPA)[168]	"(a)(3) the term 'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider…" "(d) Personally identifiable information.--Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State."

[166] Cal. Jury Instr.--Crim. 15.61, Cal. Jury Instr.--Crim. 15.61.
[167] Song-Beverly Credit Card Act of 1971, Cal. Civ. Code § 1747.08 (West).
[168] 18 U.S.C.A. § 2710 (West).

Gramm-Leach-Bliley Act of 1999 (GLBA)[169]	"(4) Nonpublic personal information (A) The term 'nonpublic personal information' means personally identifiable financial information-- (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution. (B) Such term does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of this title. (C) Notwithstanding subparagraph (B), such term-- (i) shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but (ii) shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information."
Cable Communications Policy Act of 1984[170]	"(2) For purposes of this section, other than subsection (h)-- (A) the term 'personally identifiable information' does not include any record of aggregate data which does not identify particular persons…"
HIPAA Privacy Rule[171]	"Protected Health Information. The Privacy Rule protects all 'individually identifiable health information' held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information 'protected health information (PHI).'[172] 'Individually identifiable health information' is information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual,

[169] 15 U.S.C.A. § 6809 (West).
[170] 47 U.S.C.A § 551(a)(2)(A).
[171] U.S. Dept. of Health and Human Services, Summary of the HIPAA Privacy Rule, (Last Reviewed Jul. 26, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.
[172] 45 C.F.R. § 160.103.

	and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.[173] Individually identifiable health information includes many common identifiers (*e.g.*, name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g. De-Identified Health Information. There are no restrictions on the use or disclosure of de-identified health information.[174] De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: (1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual."

[173] *Id.*
[174] 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

B. Definitions of Personal Information

Source	Personal Information
Google Privacy Policy[175]	"This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account." (emphasis added).
Cal. Civ. Code Sec. 1798.81.5(d)(1)	"(1) 'Personal information' means either of the following: (A) An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social security number. (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv) Medical information. (v) Health insurance information. (vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes. (B) A username or email address in combination with a password or security question and answer that would permit access to an online account. (2) "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional. (3) "Health insurance information" means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

[175] Google Privacy & Terms, Privacy Policy Key Terms (Last Accessed Jun. 3, 2022), https://perma.cc/524M-5UH2.

	(4) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."
Cal. Civ. Code § 1798.140(o)(1)	"(o)(1) 'Personal information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers. (B) Any categories of personal information described in subdivision (e) of Section 1798.80. (C) Characteristics of protected classifications under California or federal law. (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. (E) Biometric information. (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement. (G) Geolocation data. (H) Audio, electronic, visual, thermal, olfactory, or similar information. (I) Professional or employment-related information. (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99). (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. (2) 'Personal information' does not include publicly available information. For purposes of this paragraph, 'publicly available' means information that is lawfully made available from federal, state, or local government records. 'Publicly available' does not mean biometric information collected by a business about a consumer without the consumer's knowledge. (3) 'Personal information' does not include consumer information that is de-identified or aggregate consumer information."

California Civil Code §1798.3(a)	"The term 'personal information' means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual."
California Transactions Forms Business Transactions § 32:213.[176]	"(6) "Personal information' means any information that when it was disclosed identified, described, or was able to be associated with an individual and includes all of the following: (A) an individual's name and address; (B) electronic mail address; (C) age or date of birth; (D) names of children; (E) electronic mail or other addresses of children; (F) number of children; (G) the age or gender of children; (H) height; (I) weight; (J) race; (K) religion; (L) occupation; (M) telephone number; (N) education; (O) political party affiliation; (P) medical condition; (Q) drugs, therapies, or medical products or equipment used; (R) the kind of product the customer purchased, leased, or rented; (S) real property purchased, leased, or rented; (T) the kind of service provided; (U) Social Security number; (V) bank account number; (W) credit card number; (X) debit card number; (Y) bank or investment account, debit card, or credit card balance;

[176] 5 Cal. Transactions Forms--Bus. Transactions § 32:213.

	(Z) payment history; and (AA) information pertaining to creditworthiness, assets, income, or liabilities. [Civ. Code, § 1798.83(e)(7)].”
California Practice Guide: Privacy Law[177]	“b. [6:813] ‘Personal information’ defined: The term “personal information” means any information that is maintained by the exchange that identifies or describes an individual, including, but not limited to, any of the following: — name; — social security number; — physical description; — home address; — home telephone number; — education; — financial matters; — medical or employment history; and — statements made by, or attributed to, the individual. [Gov.C. § 100503(a)(2)(C) (incorporating by reference definition of “personal information” contained in Civ.C. § 1798.3)]”
California Transactions Forms Business Transactions - § 32:211. Destruction of records of personal information[178]	“(5) ‘Personal information’ means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information. [Civ. Code, § 1798.80(e)].”
Regulations Under Specific Acts of Congress - Part 312. Children's Online Privacy Protection Rule[179]	“Personal information means individually identifiable information about an individual collected online, including: (1) A first and last name; (2) A home or other physical address including street name and name of a city or town; (3) Online contact information as defined in this section; (4) A screen or user name where it functions in the same manner as online contact information, as defined in this section;

[177] H. Privacy of Information Maintained by California's Health Benefit Exchange, Cal. Prac. Guide Privacy Law Ch. 6-H.
[178] 5 Cal. Transactions Forms--Bus. Transactions § 32:211.
[179] 16 C.F.R. § 312.2 (2013).

	(5) A telephone number; (6) A Social Security number; (7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier; (8) A photograph, video, or audio file where such file contains a child's image or voice; (9) Geolocation information sufficient to identify street name and name of a city or town; or (10) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition."
Children's Online Privacy Protection Act (COPPA)[180]	"Personal information means individually identifiable information about an individual collected online, including: (1) A first and last name; (2) A home or other physical address including street name and name of a city or town; (3) Online contact information as defined in this section; (4) A screen or user name where it functions in the same manner as online contact information, as defined in this section; (5) A telephone number; (6) A Social Security number; (7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier; (8) A photograph, video, or audio file where such file contains a child's image or voice; (9) Geolocation information sufficient to identify street name and name of a city or town; or (10) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition."
§ 549. Definitions related to the Information Practice Act[181]	"Under the provisions governing information practices, the term "personal information" means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone

[180] 16 C.F.R. § 312.2.
[181] 13A Cal. Jur. 3d Consumer, etc. Protection Laws § 549.

	number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual."

C. Definitions of Identifying Information

Source	Identifying Information
"Privacy-Preserving Data Sharing for Medical Research," Stabilization, Safety, and Security of Distributed Systems: 23rd International Symposium[182]	"An identifier by itself is meaningless and is just a code. For example, any random combination of nine numbers very well may be a social security number, but without identifying information, there is no relevance, utility or vulnerability. Identifying information alone is not overly relevant, because it simply notes the existence of a person, without any detail of that person."
FCRA	"Notwithstanding the provisions of section 1681b of this title, a consumer reporting agency may furnish identifying information respecting any consumer, limited to his name, address, former addresses, places of employment, or former places of employment, to a governmental agency."[183] "(b) Identifying information: Notwithstanding the provisions of section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information, signed by the Director or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an

[182] Michael J. Fischer, Jonathon E. Hochman, and Daniel Boffa, "Privacy-Preserving Data Sharing for Medical Research," Stabilization, Safety, and Security of Distributed Systems: 23rd International Symposium, SSS 2021, Virtual Event, https://doi.org/10.1007/978-3-030-91081-5_6 (Nov. 17–20, 2021) ("Hochman Paper"), at 2-3.

[183] 15 U.S.C.A. § 1681f.

	investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.[184] "(3) Procedures: The request of a victim under paragraph (1) shall-- (A) be in writing; (B) be mailed to an address specified by the business entity, if any; and (C) if asked by the business entity, include relevant information about any transaction alleged to be a result of identity theft to facilitate compliance with this section including-- (i) if known by the victim (or if readily obtainable by the victim), the date of the application or transaction; and (ii) if known by the victim (or if readily obtainable by the victim), any other identifying information such as an account or transaction number."[185] "(3) Identity theft: The term "identity theft" means a fraud committed using the identifying information of another person, subject to such further definition as the Bureau may prescribe, by regulation."[186]
18 U.S.C.A § 1029	"(a)(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or… (e)(11) the term "telecommunication identifying information" means electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument."
10 CCR § 2593.2	"A query shall allow for, but is not limited to, the following identifying information on an employer to inquire about the employer's coverage information on a specified date: Name of the employer; Name of the employer and a full or partial address of the employer, including, but not limited to, street name, city, and state; or FEIN."

[184] 15 U.S.C.A. § 1681u. (emphasis added).

[185] 15 U.S.C.A. § 1681g. (emphasis added).

[186] 15 U.S.C.A. § 1681a.

11 C.F.R. § 9410.2 11	"Record means any item, collection, or grouping of information about an individual that is maintained by the Commission including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history and that contains his or her name or the identifying number, symbol, or other identifying information particularly assigned to the individual, such as finger or voice print or a photograph. Systems of records means a group of any records under the control of the Commission from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying information particularly assigned to the individual."
42 C.F.R. § 426.400	(2) If the beneficiary has a representative, the representative-identifying information must include the following: (i) Name. (ii) Mailing address. (iii) Telephone number. (iv) E–mail address, if any
5 C.F.R. § 581.203	Sufficient identifying information must accompany the legal process in order to enable processing by the governmental entity named. Therefore, the following identifying information about the obligor, if known, is requested: (1) Full name; (2) Date of birth; (3) Employment number, social security number, Department of Veterans Affairs claim number, or civil service retirement claim number; (4) Component of the governmental entity for which the obligor works, and the official duty station or worksite; and (5) Status of the obligor, *e.g.*, employee, former employee, or annuitant.
5 C.F.R. § 9301.13	b) At a minimum, the request should contain sufficient identifying information to allow SIGAR to determine if there is a record pertaining to the individual making the request in a particular system of records. In instances when the requester's identification is insufficient to ensure disclosure to the individual to whom the information pertains in view of the sensitivity of the information, SIGAR reserves the right to solicit from the person requesting access to a record additional identifying information.
34 U.S.C.A. § 12291	(20) Personally *identifying information* or personal information

	The term "personally identifying information" or "personal information" means individually identifying information for or about an individual including information likely to disclose the location of a victim of domestic violence, dating violence, sexual assault, or stalking, regardless of whether the information is encoded, encrypted, hashed, or otherwise protected, including-- (A) a first and last name; (B) a home or other physical address; (C) contact information (including a postal, e-mail or Internet protocol address, or telephone or facsimile number); (D) a social security number, driver license number, passport number, or student identification number; and (E) any other information, including date of birth, racial or ethnic background, or religious affiliation, that would serve to identify any individual.
22 U.S.C.A. § 2507a	(1) Personally identifying information The term "personally identifying information" means individually identifying information for or about a volunteer who is a victim of sexual assault, including information likely to disclose the location of such victim, including the following: (A) A first and last name. (B) A home or other physical address. (C) Contact information (including a postal, email, or Internet protocol address, or telephone or facsimile number). (D) A social security number. (E) Any other information, including date of birth, racial or ethnic background, or religious affiliation, that, in combination with information described in subparagraphs (A) through (D), would serve to identify the victim.
42 U.S.C.A. § 11360	The term "personally identifying information" means individually identifying information for or about an individual, including information likely to disclose the location of a victim of domestic violence, dating violence, sexual assault, or stalking, including-- (A) a first and last name; (B) a home or other physical address; (C) contact information (including a postal, e-mail or Internet protocol address, or telephone or facsimile number); (D) a social security number; and

	(E) any other information, including date of birth, racial or ethnic background, or religious affiliation, that, in combination with any other non-personally identifying information, would serve to identify any individual.

D. Curriculum Vitae

PAUL M. SCHWARTZ

Jefferson E. Peyser Professor of Law
U.C. Berkeley School of Law
Law School Building # 7200
Berkeley, California 94720-7200
website: www.paulschwartz.net
Email: pschwartz@law.berkeley.edu

Tel: 510-643-0352
Fax: 510-643-2673

EDUCATION:

Yale Law School, J.D., June 1985
Yale Law Journal, Volume 94, Senior Editor

Brown University, B.A. 1981, *magna cum laude*
Honors in history and English, *Phi Beta Kappa*

PUBLICATIONS
BOOKS:

PRIVACY LAW FUNDAMENTALS (IAPP, 6th ed. 2022) (Daniel J. Solove, co-author)

PRINCIPLES OF THE LAW, DATA PRIVACY, AMERICAN LAW INSTITUTE (2020) (co-reporter with Daniel J. Solove)

INFORMATION PRIVACY LAW (ASPEN PUBLISHERS, 7th ed., 2020) (Daniel J. Solove, co-author)

INFORMATION PRIVACY STATUTES AND REGULATIONS, 2010-2011 (ASPEN PUBLISHERS, 2008) (Daniel J. Solove, co-editor)

ON-LINE SERVICES, DATA PROTECTION LAW AND PRIVACY: REGULATORY RESPONSES (Official Pub.of the European Union, Brussels, 1998)(Joel R. Reidenberg, co-author). Study carried out for the Commission of the European Communities (DGXV) regarding on-line privacy in Belgium, France, Germany, and the United Kingdom.

DATA PRIVACY LAW (Michie Publishing/Lexis Law Publishing, 1996), with Joel R. Reidenberg, co-author

ARTICLES, ESSAYS, CHAPTERS:

Privacy and/or Trade, 90 UNIVERSITY OF CHICAGO LAW REVIEW -- (forthcoming 2023), with Anupam Chander, co-author

ALI Data Privacy Law: Overview and Black Letter Text, 68 U.C.L.A. Law Review 1252 (2022), with Daniel Solove, co-author

The Data Privacy Law of Brexit: Preference Formation, Transaction Costs, and Ideology, 22 Theoretical Issues in Law 111 (2021)

Global Data Privacy Law, 94 N.Y.U. LAW REVIEW 771 (2019)

Data Localization Under the CLOUD Act and the GDPR, 2019 COMPUTER LAW REVIEW INTERNATIONAL 1, with Karl-Nikolaus Peifer, co-author

Legal Access to the Global Cloud, 118 COLUMBIA LAW REVIEW 1681 (2018)

Transatlantic Data Privacy Law, 106 GEORGETOWN LAW JOURNAL 115 (2017) with Karl-Nikolaus Peifer, co-author. Selected as 2017-2018 "Privacy Paper for Policymakers" by the Future of Privacy Forum.

Systematic Government Access to Private-Sector Data in Germany, in BULK COLLECTION 61 (Fred H. Cate & James X. Dempsey, eds. Oxford University Press, 2017)

Foreword, DETERMANN'S CALIFORNIA PRIVACY LAW: PRACTICAL GUIDE AND COMMENTARY (2017)

Microsoft Ireland *and a Level Playing Field for U.S. Cloud Companies*, 15 PVLR 1549 (Aug. 1, 2016), reprinted at 16 World Data Production Report 7 (July 28, 2016)

The Value of Privacy Federalism, in SOCIAL DIMENSIONS OF PRIVACY 324 (Beate Roessler & Dorota Mokorsinska, eds., Cambridge University Press, 2015)

Reconciling Personal Information in the European Union and United States, 102 CALIFORNIA LAW REVIEW 877 (2014), with Daniel J. Solove, co-author

The EU-US Privacy Collision: A Turn to Institutions and Procedures, 126 HARVARD LAW REVIEW 1966 (2013)

Privacy in the Cloud, 161 UNIVERSITY PENNSYLVANIA LAW REVIEW 1623 (2013)

Systematic Government Access to Private-Sector Data in Germany, 2 INTERNATIONAL DATA PRIVACY LAW 289 (2012)

Reforming the concept of personally identified information: U.S. privacy law and PII 2.0 (with Daniel Solove), in NEUE REGULIERUNGSSCHUB IM DATENSCHUTZRECHT? 55 (Rolf H. Weber & Florent Thouvenin, eds.), Schulthess Verlag (Switzerland)(2012).

PII 2.0: Privacy and a New Approach to Personal Information, Privacy and Security Law Report, 11 PVLR 142 (January 10, 2012), with Daniel J. Solove, co-author

The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. LAW REVIEW 1814 (2011), with Daniel Solove, co-author

Regulating Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology, 53 WILLIAM & MARY LAW REVIEW 351 (2011)

Privacy, Ethics, and Analytics, 9 IEEE SECURITY AND PRIVACY 66 (Nr. 3, May/June 2011)

Data Protection Law and the Ethical Use of Analytics, PRIVACY AND SECURITY LAW REPORT, 10 PVLR 70 (January 10, 2011)

Prosser's Privacy *and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept, 98* CALIFORNIA LAW REVIEW *1925* (2010), with Karl-Nikolaus Peifer, co-author

Managing Global Data Privacy, 10 PRIVACY ADVISOR 14 (Number 1, Jan.-Feb. 2010)

Preemption and Privacy: Against a Federal Privacy Law, 118 YALE LAW JOURNAL 902 (2009)

Warrantless Wiretapping, FISA Reform, and the Lessons of Public Liberty: A Comment on Holmes' Jorde Lecture, 97 CALIFORNIA LAW REVIEW 407 (2009)

From Victorian Secrets to Cyberspace Shaming, Review Essay, 76 UNIVERSITY OF CHICAGO LAW REVIEW 1407 (2009)

Keeping Track of Telecommunications Surveillance, 52 COMMUNICATIONS OF THE ACM 24 (Sept. 2009)

The Future of Tax Privacy, 62 NATIONAL TAX JOURNAL 883 (2008)

Reviving Telecommunications Surveillance Law, 75 UNIVERSITY OF CHICAGO LAW REVIEW 287 (2008)

Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches, 75 UNIVERSITY OF CHICAGO LAW REVIEW 261 (2008), with Ira S. Rubinstein and Ronald D. Lee, co-authors

Anonymous Disclsoure of Security Breaches, with Edward J. Janger, co-author, in SECURING PRIVACY IN THE INTERNET AGE 221 (Anupam Chandler, Lauren Gelman & Margaret Jane Raden, eds., Stanford Law Books, 2008)

Technological Change: Networked Intelligence and Information Privacy, with Ronald D. Lee, co-author, in CIVIL LIBERTIES AND NATIONAL SECURITY: A HISTORICAL PERSPECTIVE 189 (Daniel Farber, ed., Russell Sage Foundation, 2008)

Notification of Data Security Breaches, 105 MICHIGAN LAW REVIEW 913 (2007), with Edward J. Janger, co-author

Privacy Inalienability and Personal Data Chips, in PRIVACY AND IDENTITY: THE PROMISE AND PERILS OF A TECHNOLOGICAL AGE (Katherine Strandburg & Daniela Stan Raicu, editors, Springer 2006)(abridged version of *Property, Privacy, and Personal Data*)

Review*, Beyond the War in Terrorism: Towards the New Information Network,*
(*Reviewing* PHILIP HEYMANN, TERRORISM, FREEDOM, AND SECURITY: WINNING WITHOUT WAR (2003), with Ronald D. Lee, co-author, 103 MICHIGAN LAW REVIEW 1446 (2005)

Privacy Inalienability and the Regulation of Spyware, 20 BERKELEY TECHNOLOGY LAW JOURNAL 1269 (2005)

Property, Privacy, and Personal Data, 117 HARVARD LAW REVIEW 2055 (2004)

Evaluating Telecommunications Surveillance in Germany: The Lessons of the Max Planck Institute Study, 73 GEORGE WASHINGTON LAW REVIEW 1244 (2004)

Lochner and *Eldred*: *Copyright Term Extension and Intellectual Property as Constitutional Property,* with William M. Treanor, co-author, 112 YALE LAW JOURNAL 2331 (2003)

Review, *The New Privacy, Oversight of the Poor, and Total Information Awareness* (Reviewing JOHN GILLIOM, OVERSEERS OF THE POOR:

SURVEILLANCE, RESISTANCE AND THE LIMITS OF PRIVACY (2001)), with William Treanor, co-author, 101 MICHIGAN LAW REVIEW 2163 (2003)

German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance, 54 HASTINGS LAW JOURNAL 751 (2003)

Voting Technology and Democracy, 77 NEW YORK UNIVERSITY LAW REVIEW 625 (2002)

The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules, with Edward J. Janger, co-author, 86 MINNESOTA LAW REVIEW 1219 (2002)

Vote.com and Internet Politics: A Comment on Dick Morris's Version of Internet Democracy, 34 LOYOLA L.A. LAW REVIEW 1071 (2001)

Testimony, Senate Committee on Commerce, Science and Transportation, Hearing on Internet Privacy, July 11, 2001

Beyond Lessig's CODE *for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WISCONSIN LAW REVIEW 743

Comment, *Free Speech versus Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STANFORD LAW REVIEW 1559 (2000)

Internet Privacy and the State, 32 CONNECTICUT LAW REVIEW 815 (2000). Lead article in symposium issue of the CONNECTICUT LAW REVIEW; the issue also contains five responses to my article.

Charting a Privacy Research Agenda: Responses, Agreements, and Reflections, 32 CONNECTICUT LAW REVIEW 929 (2000). Responding to the five scholars who commented on my article, *Internet Privacy and the State*.

Democracy and Privacy in Cyberspace, 52 VANDERBILT LAW REVIEW 1609 (1999)

Privacy and the Economics of Personal Health Care Information, 76 TEXAS LAW REVIEW 1 (1997)

European Data Protection Law and Medical Privacy, in GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 392 (Mark A. Rothstein, ed., Yale University Press, 1997)

Privacy and Participation: Personal Information and Public Sector Regulation in the United States, 80 IOWA LAW REVIEW 533 (1995)

European Data Protection Law and Restrictions on International Data Flows, 80 IOWA LAW REVIEW 471 (1995)

The Protection of Privacy in Health Care Reform, 48 VANDERBILT LAW REVIEW 295 (1995)

Constitutional Change and Constitutional Legitimation: The Example of German Unification, 31 HOUSTON LAW REVIEW 1027 (1994)

Testimony to Government Information, Justice, Transportation, and Agriculture Subcommittee of House Committee on Government Operations, House of Representatives, 103rd Congress, *reprinted in* FAIR HEALTH INFORMATION PRACTICES ACT OF 1994 (2d Session on H.R. 4077) 358 (1994)

Data Processing and Government Administration: The Failure of the American Legal Response to the Computer, 43 HASTINGS LAW JOURNAL 1321 (1992)

Book Review, *The Oversight of Data Protection*, 39 AMERICAN JOURNAL OF COMPARATIVE LAW 618 (1991)

Review Essay, *Baby M. in West Germany*, 89 COLUMBIA LAW REVIEW 347 (1989)

The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, 37 AMERICAN JOURNAL OF COMPARATIVE LAW 675 (1989)

Note, *Parental Rights and the Habilitation Decision for Mentally Retarded Children*, 94 YALE LAW JOURNAL 1715 (1985)

SHORTER WORKS- COLUMNS & OP-EDS:

Foreward, Determann's California Privacy Law: Practical Guide and Commentary (4th ed., 2020)

Preface: Privacy Law in the Pandemic Year
Korean Legislation Research Institute, Issue Brief: Data Protection (October 2020)

Illusions of consent and COVID-19 tracking apps
IAPP Privacy Perspectives (May 19, 2020)

Protecting privacy on COVID-19 surveillance apps
IAPP Privacy Perspectives (May 8, 2020)

Microsoft Ireland and a Level Playing Field for U.S. Cloud Companies 15 PVLR 1549 (Aug. 1, 2016), reprinted at 16 World Data Production Report 7 (July 28, 2016)
The Delayed Revolution in Digital Financial Services, TechCrunch.com (April 9, 2016)

Risk and High Risk: Walking the GDPR Tightrope, IAPP Privacy Perspectives (March 29, 2016)

Navigating the cloud: key regulatory issues to know, DAILY JOURNAL, ASIA SUPPLEMENT (Oct. 22, 2014), with Behnam Dayanim

Defining "Personal Data" in the European Union and United States, 13 PVLR 1581 (Sept. 15 2014) with Daniel J. Solove, co-author, reprinted at 14 WORLD DATA PROTECTION REPORT 4 (Sept. 2014)

Differing Privacy Regimes: A Mini-Poll on Mutual EU-U.S. Distrust, IAPP PRIVACY PERSPECTIVES (July 22, 2014)

The Battle for Leadership in Education Privacy Law, SAFEGOV.ORG (Mar. 27, 2014) with Daniel Solove

In Practice: The 'California Effect' on Privacy Law, THE RECORDER, Jan. 2, 2014

Testimony, Balancing Privacy and Opportunity in the Internet Age, California Assembly Informational Hearing, Dec. 12, 2013

Blog, What Is Personally Identifiable Information (PII)? Finding Common Ground in the EU and US, CONCURRING OPINIONS (June 26, 2013) with Daniel Solove

EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation, 12 PVLR 718 (Apr. 28, 2013)

Privacy Firsts at Berkeley Law, SAN FRANCISCO CHRONICLE E5 (Feb. 25, 2012)
Blog, *PII 2.0*, TECHNOLOGY|POLICY|ACADEMICS (Jan. 16, 2012) with Daniel Solove

Blog, *Google Ngram and Information Privacy*, GOOGLE POLICY BY THE NUMBERS (Jan. 9, 2012)(Daniel J. Solove, co-author)

Amend telecommunications surveillance laws, SAN FRANCISCO CHRONICLE H6 (March 1, 2009)

Essay, *Bye to chads; hello to what?*, NATIONAL LAW JOURNAL A24 (June

11, 2001)

Book Review, The Lawyer's Bookshelf: You Say You Want a Revolution, By Reed E. Hundt (2000), NEW YORK LAW JOURNAL 2 (July 10, 2000)

Book Review, The Lawyer's Bookshelf: The Code Book, By Simon Singh (1999), NEW YORK LAW JOURNAL 2 (Dec. 21, 1999)

American Data Protection Law Today, RECUEIL DES COMMUNICATIONS/ COLLECTION OF PAPERS, Twelfth Annual Conference of Data Protection Commissioners (France, 1990), *reprinted in* TRANSNATIONAL DATA REPORT 20 (Netherlands 1990); Privacy Laws & Business 11 (October 1990) (England); and XII Conférence Internationale des Commissaires à la Protection des Données (France, 1990) (French translation)

Recent Public Trends in West Germany, PARTISAN REVIEW 235 (1987). Analysis of a debate among German historians about the contemporary meaning of the Holocaust.

GERMAN LANGUAGE PUBLICATIONS:

Datentreuhändermodelle – Sicherheit vor Herausgabeverlangen US-amerikanischer Behörden und Gerichte?, COMPUTER UND RECHT 165 (3/2017) ("Data Fiduciary Model – Protection from Data Requests of U.S. Governmental Authorities and Courts?") with Karl-Nikolaus Peifer

Zur Architektonik des Datenschutzes in den U.S.A., in DATENSCHUTZ IM DIGITALEN ZEITALTER – GLOBAL, EUROPÄISCH, NATIONAL (2015) ("The Architecture of Data Protection in the USA," in Data Protection in the Digital Age: Global, European, National)

Referat, in Verhandlung des 69. Deutschen Juristentages: München 2012, Band II/1, O73 (2013) (Presentation, in Proceedings of the 69th German Jurists' Forum)

"Personenbezogene Daten" aus internationaler Perspektive, (An International Perspective on "Personal Data"), ZEITSCHRIFT FÜR DATENSCHUTZ 97 (March 20, 2011)

Kehrtwende beim Datenschutz (Turning Point for Data Protection Law)(translation Al Sopot), BERLIN TAGESSPIEGEL, Sept. 5, 2002 (op-ed about privacy developments after 9/11)

Das Übersetzen im Datenschutz: Unterschiede zwischen deutschen und amerikanischen Konzepten der "Privatheit" (Translating the Legal Concept

of "Privacy": Differences between American and German Approaches), 8 RECHT DER DATENVERARBEITUNG 8 (1992), *reprinted in* ÜBERSETZEN, VERSTEHEN, BRÜCKEN BAUEN (Erich Schmidt Press, Berlin, 1993)

Die neuesten Entwicklungen im amerikanischen Datenschutzrecht (New Trends in American Data Protection Law), 5 RECHT DER DATENVERARBEITUNG 153 (1989)

EXPERT WITNESS & CONSULTING:

Expert cases include Gerling Global Reinsurance Corp v. Quackenbush, 2000 WL 777978 (E.D. Cal. 2002), *reversed* American Ins. Ass'n v. Garamendi, 539 U.S. 396 (2003). Worked on this case as part of an international team of lawyers assisting the State of California in defense of the Holocaust Insurance Relief Act (HIVRA). State statute required insurance companies to disclose to the State of California any involvement with insurance policies of Holocaust victims. Provided affidavits and advice to California regarding German information privacy law and whether it prohibited compliance with HIVRA.

Other reported opinions on cases on which I worked as expert include: In re: Vitamins Antitrust Litigation, 2001 WL 1049433 (D.D.C. 2001); and VWAG v. Monceaux, 909 S.W. 2d 900 (Texas 1995).

Past clients include the Commission of the European Union, the State of California, Volkswagen AG, and other multinational corporations.

GRANTS AND AWARDS:

American Academy in Berlin, Berlin Prize Fellow, Germany, Fall 2002; German Marshall Fund, Transatlantic Fellow, Transatlantic Center, Brussels, Belgium, Spring 2003: Funded Research Project*: Post 9-11 Developments in Telecommunications Privacy Law in the U.S., Germany, and the European Union*

Other Grants and Awards: Thyssen Foundation, 2012 (with University of Cologne Law School); German Academic Exchange Award, 1997; Harry Frank Guggenheim Foundation Fellowship, Spring 1995; Fulbright Scholarship, 1991; Alexander von Humboldt Scholar, 1986-1988.

ADVISORY BOARDS:

Brussels Privacy Hub, Vrije University Brussels, Belgium, Advisory Board Member

INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY, Oxford University Press, Editorial Board Member

INTERNATIONAL DATA PRIVACY LAW, Oxford University Press, Editorial Board Member

ZEITSCHRIFT FÜR DATENSCHUTZ (Data Protection Journal), Editorial Board Member

Future of Privacy Forum, Washington D.C., Board of Advisors

Trusted Computing Academic Advisory Board, (TCAAB), Microsoft Corporation, Redmond, Washington (Member, 2003-2011). The TWCAAB advised Microsoft on its trusted computing initiative and other policy and computing issues.

PROFESSORSHIPS AND ACADEMIC POSITIONS:

Co-Reporter, Data Privacy Principles Project, American Law Institute, 2013 to 2020. Project approved May 2019 by ALI, finalized and published December 2020

Jefferson E. Peyser Professor of Law, University of California-Berkeley School of Law, Boalt Hall, 2014 to present

Professor of Law, University of California-Berkeley School of Law, Boalt Hall, 2006-2014

Anita and Stuart Subotnick Professor of Law, Brooklyn Law School, 2004-2006; Professor of Law, Brooklyn Law School, 1998-2004.

Professor of Law, University of Arkansas School of Law (Fayetteville), Fall 1995- Spring 1998. Associate Professor, 1992-1995, Assistant Professor, 1988- 1992.

Guest Scholar, Institute for Labor, Economic and Civil Law, Goethe University, Frankfurt/Main, Germany, Summer 1998, Summer 1997, Summer 1996, Summer 1995, Summer 1993, Summer 1992, Summer 1991, Summer 1990, Summer 1989.

Guest Professor, University of Nantes, School of Law & Political Science, Nantes, France, Summer 1993, Summer 1992.

MEMBERSHIP, PROFESSIONAL SOCIETIES:

American Law Institute, Elected 2005
New York Bar, Admitted September 2014
Arkansas Bar, Admitted February 1988

German Academic Exchange Alumni Association
Alexander von Humboldt Foundation Alumni Association
Phi Beta Kappa, Brown University, 1981

E. Court Testimony in the Last Four Years

- Expert Legal Opinion of Professor Paul M. Schwartz in the case entitled *Barak v. Facebook Ireland Limited*, Case No. 32672-02-17, pending in the District Court in Tel Aviv, Israel, March 14, 2019.

- Expert Opinion of Professor Paul M. Schwartz in the case entitled *Calhoun v. Google*, Case No. 4:20-cv-05146-YGR-SVK, pending in the Northern District of California, January 22, 2022.

F. Materials Considered

Filed Documents:

- Third Amended Complaint (Dkt. 395-2)
- Declaration. of Alexei Svitkine (Dkt. 112-5)
- Report of Dr. Zubair Shafiq, *Calhoun v. Google*, 5:20-cv-05146-LHK, (Dkt. 340-19)
- Declaration of David Monsees, *Calhoun v. Google*, 5:20-cv-05146-LHK, (Dkt. No. 428-22)

Public Documents:

- J. Hochman, M. Fischer and D. Boffa Privacy-Preserving Data Sharing for Medical Research, Yale University (2021)
- Michael J. Fischer, Jonathon E. Hochman, and Daniel Boffa, "Privacy-Preserving Data Sharing for Medical Research," Stabilization, Safety, and Security of Distributed Systems: 23rd International Symposium, SSS 2021, Virtual Event, https://doi.org/10.1007/978-3-030-91081-5_6 (Nov. 17–20, 2021)
- Paul M. Schwartz & Daniel J. Solove, Reconciling Personal Information in the United States and European Union (2014)
- Paul M. Schwartz & Daniel J. Solove, Defining "Personal Data" in the European Union and U.S. (2014)
- Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information (2011)
- Paul M. Schwartz, "Personenbezogene Daten" aus internationaler Perspektive, Zeitschrift für Datenschutz 97 (3/2011) ("Personal-specific Data" from an International Perspective)
- Federal Trade Commission (F.T.C.) Report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers" (March 26, 2012)
- In the Matter of Protecting the Privacy of Customers of Broadband & Other Telecommunications Services, WC Docket No. 16-106, Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission (May 27, 2016), https://perma.cc/2EJZ-ENW8
- Christina H. Kroll, CCPA: The California Senate is Not Ready to Expand the Consumer Right of Action Proskauer Priv. L. Blog (May 17, 2019), https://perma.cc/699Z-QENL
- Platforms Program Policies, Google Help Center, (Last Updated Apr. 1, 2022), https://perma.cc/7D86-XR54

- Best Practices to Avoid Sending Personally Identifiable Information (PII), Analytics Help Center, (2021), https://perma.cc/L7LG-CG7W
- Prabhakar Raghavan, Raising the Bar on Transparency, Choice and Control in Digital Advertising, (May 7, 2019), Google Ads & Commerce Blog, https://perma.cc/HQH3-PPBE
- The Privacy Sandbox, Chromium Blog, https://perma.cc/7GGQ-7YV7 (last accessed Jun. 4, 2022)
- Justin Schuh, Building a more private web: A path towards making third party cookies obsolete, Chromium Blog, (Jan. 14, 2020), https://perma.cc/8LCF-7N4A
- Policy Against Fingerprints and Locally Shared Objects, Google Analytics Help Center, https://perma.cc/V44X-GEZK (2022)
- Interoperability guidance for vendors working with Google via the IAB TCFv2.0, Google Ad Manager Help Center, https://perma.cc/EC8S-MVJK (2022)
- Requirements for third-party ad serving, Google Advertising Policies Help, https://perma.cc/JP2W-8H7Z (2022)
- Federal Trade Commission (F.T.C.), Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 26, 2012)
- Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, at 18-20 (March 26, 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
- Understanding PII in Google's Contracts and Policies, Google Help Center, (2021), https://support.google.com/analytics/answer/7686480
- U.S. Department of Labor, Guidance on the Protection of Personal Identifiable Information, (last visited Dec. 21, 2021), https://www.dol.gov/general/ppii
- National Institute of Standards and Technology, Glossary: Personally Identifiable Information (PII), (last visited Dec. 21, 2021), https://csrc.nist.gov/glossary/term/personally_identifiable_information
- Ferraiolo, et al., Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI) at 46, (July 2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-79-2.pdf
- Ross, et al., Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy at 1, (December 2018), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
- Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016
- Simson L. Garfinkel, De-Identification of Personal Information at 42-43, (October 2015), https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf
- GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, (May 2008), http://www.gao.gov/new.items/d08536.pdf
- U.S. General Services Administration, Rules and Policies - Protecting PII - Privacy Act, (Last Reviewed Jan. 12, 2020), https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act
- Beth Anne Killoran, U.S. General Services Administration, 2180.2 CIO GSA Rules of Behavior for Handling Personally Identifiable Information (PII), (Oct. 19, 2019),

https://www.gsa.gov/directive/gsa-rules-of-behavior-for-handling-personally-identifiable-information-(pii)-

- Mobile Tech. Mgmt., US DOE 203.2 (May 15, 2014), https://www.energy.gov/sites/default/files/2015/08/f25/o203.2.pdf
- Minor Changes to Doe O 206.1, Dep't of Energy Priv. Program, US DOE 206.1 (Nov. 1, 2018), https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder-chg1-minchg/@@images/file
- Prot. of Hum. Rsch. Subjects, US DOE 443.1C at 20 (Nov. 26, 2019). https://www.directives.doe.gov/directives-documents/400-series/0443.1-BOrder-c/@@images/file at 20
- U.S. Dept. of Commerce, Safeguarding Information, (last updated Oct. 1, 2021), https://www.osec.doc.gov/opog/privacy/pii_bii.html.
- U.S. Dept. of Education, Protecting Student Privacy, (Last Visited Dec. 21, 2021), https://studentprivacy.ed.gov/content/personally-identifiable-information-pii.
- Family Educational Rights and Privacy Act Regulations, 34 CFR §99.3 https://www.ecfr.gov/current/title-34/subtitle-A/part-99,
- 20 U.S.C. 1232g, https://www.govinfo.gov/content/pkg/USCODE-2019-title20/pdf/USCODE-2019-title20-chap31-subchapIII-part4-sec1232g.pdf), (Last Visited Dec. 21, 2021)
- California Business and Professions Code §22577(a) https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22577, (Last Visited Jun. 4, 2022)
- Google Privacy & Terms, Privacy Policy Key Terms (Last Accessed Jun. 3, 2022), https://perma.cc/524M-5UH2
- U.S. Dept. of Health and Human Services, Summary of the HIPAA Privacy Rule, (Last Reviewed Jul. 26, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
- App. C (42 C.F.R. § 426.400, 5 C.F.R. § 581.203, 34 U.S.C.A. § 12291, 22 U.S.C.A. § 2507a, 42 U.S.C.A. § 11360)
- General Data Protection Regulation, Article 4 (European Union)
- ALI Data Privacy Principles
- CCPA § 1798.140(v)(1)
- CCPA § 1798.81.5(d)(1)
- CCPA § 1798.140(o)(1)
- CCPA § 1798.81.5(d)(1)
- Cal. Civ. Code § 1798.140(o)
- Cal. Civ. Code § 1798.155(b)
- California Consumer Privacy Act of 2018: Consumer Remedies, CA Sen. Bill. 561 (2019)
- Cal. Civ. Code § 1798.150(a)(1)
- Cal. Civ. Code § 1798.81.5(d)(1)
- Cal. Civ. Code § 1798.140(o)(1)
- Cal. Civ. Code § 1798.145(a)
- Cal. Civ. Code, §1798.140(o)(3)
- Cal. Civ. Code § 1798.140(r)
- Cal. Civ. Code § 1798.145(p)

- Cal. Civ. Code § 1798.145(j)
- 2 CFR § 200.79, https://perma.cc/P9HC-XF2U
- 2 CFR § 200.338, https://perma.cc/8E4S-2XMY
- 2 CFR § 200.1
- 2 C.F.R. § 200.1 (2021)
- E–GOVERNMENT ACT OF 2002, PL 107–347, December 17, 2002
- Cal. Penal Code § 530.55 (West 2007)
- Cal. Jury Instr.--Crim. 15.61, Cal. Jury Instr.--Crim. 15.61
- Song-Beverly Credit Card Act of 1971, Cal. Civ. Code § 1747.08 (West)
- 18 U.S.C.A. § 2710 (West)
- 15 U.S.C.A. § 6809 (West)
- 47 U.S.C.A § 551(a)(2)(A)
- 45 C.F.R. § 160.103
- 20 U.S.C. §1232g
- 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b)
- Cal. Civ. Code Sec. 1798.81.5(d)(1)
- Cal. Civ. Code § 1798.140(o)(1)
- 20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99
- California Civil Code §1798.3(a)
- 5 Cal. Transactions Forms--Bus. Transactions § 32:213
- Gov.C. § 100503(a)(2)(C)
- Civ.C. § 1798.3
- H. Privacy of Information Maintained by California's Health Benefit Exchange, Cal. Prac. Guide Privacy Law Ch. 6-H
- 5 Cal. Transactions Forms--Bus. Transactions § 32:211
- 16 C.F.R. § 312.2 (2013)
- 13A Cal. Jur. 3d Consumer, etc. Protection Laws § 549
- 15 U.S.C.A. § 1681f
- 18 U.S.C.A § 1029
- 10 CCR § 2593.2
- 11 C.F.R. § 9410.2
- 15 U.S.C.A. § 1681u
- 15 U.S.C.A. § 1681g
- 15 U.S.C.A. § 1681a
- 42 C.F.R. § 426.400
- 5 C.F.R. § 581.203
- 5 C.F.R. § 9301.13
- 34 U.S.C.A. § 12291
- 22 U.S.C.A. § 2507a
- 42 U.S.C.A. § 11360

Expert Reports:

- Hochman Report
- Schneier Report
- Psounis Rebuttal Report
- Zervas Rebuttal Report

Produced Documents:

- GOOG-CALH-00027147
- GOOG-CABR-04400013
- GOOG-CALH-00027147
- GOOG-BRWN-00029004
- GOOG-BRWN-00029004
- GOOG-CABR-00073880